Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

Series/Number:	NIST Special Publication 800-126
Title:	The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0
Publication Date(s):	November 2009
Withdrawal Date:	November 27, 2018
Withdrawal Note:	SCAP v1.0 is no longer supported. For the latest SCAP releases, see https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases

Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	
Title:	
Author(s):	
Publication Date(s):	
URL/DOI:	

Additional Information (if applicable)

Contact:	Computer Security Division (Information Technology Laboratory)
Latest revision of the attached publication:	SP 800-126 Revision 3 and SP 800-126A
Related information:	https://scap.nist.gov https://csrc.nist.gov/publications/detail/sp/800-126/rev-3/final
Withdrawal announcement (link):	N/A

Date updated: November 27, 2018

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-126

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0

Recommendations of the National Institute of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart

NIST Special Publication 800-126

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0

Recommendations of the National Institute of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

November 2009

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Patrick D. Gallagher, Deputy Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-126
Natl. Inst. Stand. Technol. Spec. Publ. 800-126, 63 pages (Nov. 2009)

Acknowledgments

The authors, Stephen Quinn, David Waltermire, Christopher Johnson, Karen Scarfone, and John Banghart of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Paul Bartock of the National Security Agency (NSA); David Niemoller, Shane Shaffer, Matt Kerr, and Greg Witte of G2; Andy Bove of SecureAcuity; Jim Ronayne of Cobham; Paul Cichonski, Angela Orebaugh, and Victoria Thompson of Booz Allen Hamilton; and Jon Baker and Drew Buttner of the MITRE Corporation for their keen and insightful assistance throughout the development of the document. The authors also give a special acknowledgment to Matt Barrett of G2 for his outstanding contributions to the early drafts of the publication.

Trademark Information

Table of Contents

List of Tables

List of Figures

Executive Summary

The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information. SCAP is a multi-purpose protocol that supports automated vulnerability checking, technical control compliance activities, and security measurement. Goals for the development of SCAP include standardizing system security management, promoting interoperability of security products, and fostering the use of standard expressions of security content.

This document defines the technical composition of SCAP Version 1.0 as comprised of six specifications—eXtensible Configuration Checklist Description Format (XCCDF), Open Vulnerability and Assessment Language (OVAL®), Common Platform Enumeration (CPE™), Common Configuration Enumeration (CCE™), Common Vulnerabilities and Exposures (CVE™), and Common Vulnerability Scoring System (CVSS)—and their interrelationships. These specifications are grouped into the following three categories:

- **Languages.** The SCAP languages provide standard vocabularies and conventions for expressing security policy, technical check mechanisms, and assessment results.
- **Enumerations.** Each SCAP enumeration defines a standard nomenclature (naming format) and an official dictionary or list of items expressed using that nomenclature. For example, CVE provides a dictionary of publicly known information security vulnerabilities and exposures.[1]
- **Vulnerability measurement and scoring systems.** In SCAP, this refers to evaluating specific characteristics of a vulnerability and, based on those characteristics, generating a score that reflects the vulnerability's severity.

SCAP utilizes software flaw and security configuration standard reference data, also known as *SCAP content*. This reference data is provided by the National Vulnerability Database (NVD),[2] which is managed by NIST and sponsored by the Department of Homeland Security (DHS).

This publication defines SCAP Version 1.0 in terms of both its component specifications and the requirements for SCAP content, and also describes the details of how the elements of SCAP interoperate. The technical specification describes the requirements and conventions that are to be employed to ensure the consistent and accurate exchange of SCAP content and the ability to reliably use the content with SCAP validated tools.

The U.S. Federal Government, in cooperation with academia and private industry, is adopting SCAP and encourages its use in support of security automation activities and initiatives.[3] SCAP is achieving widespread adoption by major software and hardware manufacturers and has become a significant component of large information security management and governance programs. The protocol is expected to evolve and expand in support of the growing needs to define and measure effective security controls, assess and monitor ongoing aspects of that information security, and successfully manage systems in accordance with risk management frameworks such as NIST Special Publication 800-53[4], Department of Defense (DoD) Instruction 8500.2, and the Payment Card Industry (PCI) framework.

---

1 http://cve.mitre.org/

2 The National Vulnerability Database can be found at http://nvd.nist.gov/.

3 Refer to http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf.

4 The Risk Management Framework is described in Section 3.0 of NIST Special Publication 800-53, available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf.

By detailing the specific and appropriate usage of the SCAP 1.0 components and their interoperability, NIST encourages the creation of reliable and pervasive SCAP content and the development of a wide array of tools that leverage SCAP capabilities. The use cases described in this document do not represent an exhaustive list of all possible applications of SCAP.

Organizations that use SCAP 1.0 or develop SCAP 1.0-based content or tools should implement the following recommendations:

Follow the requirements listed in this document and in the associated component specifications.

Organizations should ensure that their use of SCAP 1.0 is compliant with the requirements detailed in each component specification and the information presented in this document. If requirements are in conflict between component specifications, this document will provide clarification. If a component specification is in conflict with this document, the requirements in this document take precedence.

When creating SCAP content, adhere to the conventions specified in this document.

Security products and checklist authors assemble content from SCAP data repositories to create viable SCAP-expressed security guidance. A security configuration checklist that documents desired security configuration settings, installed patches, and other system security elements using SCAP in a standardized format is known as an SCAP-expressed checklist. Such a checklist would use XCCDF to describe the checklist, CCE to identify security configuration settings to be addressed or assessed, and CPE to identify platforms for which the checklist is valid. The use of CCE and CPE entries within XCCDF checklists is an example of an SCAP convention—a requirement for valid SCAP usage. These conventions are considered part of the definition of SCAP 1.0. Organizations producing SCAP content should adhere to these conventions to ensure the highest degree of interoperability.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

This document provides the definitive technical specification for Version 1.0 of the Security Content Automation Protocol (SCAP). SCAP (pronounced S-CAP) consists of a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. This document describes the basics of the SCAP component specifications and their interrelationships, the characteristics of SCAP content, as well as SCAP requirements not defined in the individual component specifications.

The scope of this document is limited to SCAP Version 1.0. Other versions of SCAP and the component specifications, including emerging specifications and future versions of SCAP, are not addressed here. Future versions of SCAP will be defined in distinct revisions of this document, each clearly labeled with a document revision number and the appropriate SCAP version number.

1.3 Audience

This document is intended for three primary audiences:

- Content authors and editors seeking guidance to ensure that the SCAP content they produce operates correctly, consistently, and reliably in SCAP tools.
- Software developers and system integrators seeking to create, use, or exchange SCAP content in their products or service offerings.
- Content and/or tool developers preparing for SCAP validation at an accredited independent testing laboratory.

1.4 Document Structure

The remainder of this document is organized into the following four major sections:

- Section 2 defines SCAP 1.0 and explains the purpose of SCAP.
- Section 3 presents basic information on the specifications comprising SCAP 1.0.
- Section 4 defines conventions and requirements for using SCAP to achieve interoperability of content and tools.
- Section 5 presents use cases that demonstrate effective and compliant implementations of SCAP.

The document also contains appendices with supporting material:

- Appendix A contains an acronym and abbreviation list.
- Appendix B lists references and other resources related to SCAP 1.0 and its component specifications.
- Appendix C documents several SCAP extensions to the XCCDF component.
- Appendix D provides an example of an SCAP data stream.

1.5 Document Conventions

Some of the requirements and conventions used in this document reference XML content. These references come in two forms, inline and indented. An example of an inline reference is

"A `<cpe_dict:cpe-item>` may contain `<cpe_dict:check>` elements that reference OVAL definitions".

In this example the notation `<cpe_dict:cpe-item>` can be replaced by the more verbose equivalent "the XML element whose qualified name is `cpe_dict:cpe-item`". An even more verbose equivalent is "the XML element in the namespace '*http://cpe.mitre.org/dictionary/2.0*' whose local name is `cpe-item`".

An example of an indented reference is:

> "References to OVAL definitions are expressed using the following format:
>
> `<cpe_dict:check system=`
> `"http://oval.mitre.org/XMLSchema/oval-definitions-5"`
> `href="Oval_URL">[Oval_inventory_definition_id]</cpe_dict:check>`".

Indented references are intended to represent the form of actual XML content. Indented references represent literal content by the use of a `fixed-length font`, and parametric (freely replaceable) content by the use of an *italic font*. Square brackets '`[]`' are used to designate optional content. Thus "`[Oval_inventory_definition_id]`" designates optional parametric content.

Both inline and indented forms use qualified names to refer to specific XML elements. A qualified name associates a named element with a namespace. The namespace identifies the specific XML schema that defines (and consequently may be used to validate) the syntax of the element instance. A qualified name declares this schema to element association using the format '*prefix*:*element-name*'. The association of prefix to namespace is defined in the metadata of an XML document and generally will vary from document to document. In this specification, the conventional mappings listed in Table 1-1 are used.

Table 1-1. Conventional XML Mappings

Prefix	Namespace URI	Schema
cpe_dict	http://cpe.mitre.org/dictionary/2.0	CPE Dictionaries
cpe	http://cpe.mitre.org/language/2.0	Embedded CPE references
nvd	http://scap.nist.gov/schema/feed/vulnerability/2.0	Base schema for NVD data feeds
cve	http://scap.nist.gov/schema/vulnerability/0.4	NVD/CVE data feed elements and attributes
cvss	http://scap.nist.gov/schema/cvss-v2/0.2	NVD/CVSS data feed elements and attributes
dc	http://purl.org/dc/elements/1.1/	Simple Dublin Core elements
xccdf	http://checklists.nist.gov/xccdf/1.1	XCCDF policy documents
xml	http://www.w3.org/XML/1998/namespace	Common XML attributes
oval	http://oval.mitre.org/XMLSchema/oval-common-5	Common OVAL elements and attributes
oval-def	http://oval.mitre.org/XMLSchema/oval-definitions-5	OVAL definitions
xxxx-def	http://oval.mitre.org/XMLSchema/oval-definitions-5#*xxxx*	OVAL elements and attributes specific to an OS, Hardware or Application type *xxxx*[5]
oval-res	http://oval.mitre.org/XMLSchema/oval-results-5	OVAL results
oval-sc	http://oval.mitre.org/XMLSchema/oval-system-characteristics-5	OVAL system characteristics
xxxx-sc	http://oval.mitre.org/XMLSchema/oval-system-characteristics-5#*xxxx*	OVAL system characteristic elements and attributes specific to an OS, Hardware or Application type *xxxx*
oval-var	http://oval.mitre.org/XMLSchema/oval-variables-5	The elements, types, and attributes that compose the core schema for encoding OVAL Variables. This schema is provided to give structure to any external variables and their values that an OVAL definition is expecting.
sch	http://purl.oclc.org/dsdl/schematron	Schematron validation scripts
ds	http://www.w3.org/2000/09/xmldsig#	Interoperable XML digital signatures

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in Request for Comments (RFC) 2119.[6]

[5] The types supported by OVAL 5.3 include the AIX, CATOS, ESX, FREE BSD, HP-UX, IOS, LINUX, PIXOS, SOLARIS, UNIX, WINDOWS, INDEPENDENT (common) operating systems, and APACHE application.

[6] RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, is available at http://www.ietf.org/rfc/rfc2119.txt.

2. Overview of SCAP 1.0

NIST Special Publication (SP) 800-117, *Guide to Adopting and Using the Security Content Automation Protocol*,[7] defines the SCAP as being comprised of two major elements. [BAR09] First, SCAP is a protocol—a suite of six specifications that standardize the format and nomenclature by which security software communicates information about publicly known software flaws and security configurations annotated with common identifiers and embedded in XML. Second, SCAP also utilizes software flaw and security configuration standard reference data, also known as *SCAP content*. This reference data is provided by the National Vulnerability Database (NVD),[8] which is managed by NIST and sponsored by the Department of Homeland Security (DHS). SCAP can be used for several purposes, including automating vulnerability checking, technical control compliance activities, and security measurement. The U.S. Federal Government, in cooperation with academia and private industry, is adopting SCAP and is encouraging widespread support of it.

This document defines Version 1.0 of SCAP in terms of both its component specifications and the requirements for SCAP content. As stated in the Executive Summary, organizations that use SCAP 1.0 should ensure that their use of it is compliant with the requirements detailed in each component specification and the information presented in this document. If requirements are in conflict between component specifications, this document will provide clarification. If a component specification is in conflict with this document, the requirements in this document take precedence.

SCAP 1.0 uses the following specifications:

- Extensible Configuration Checklist Description Format (XCCDF) 1.1.4, a language for authoring security checklists/benchmarks and for reporting results of checklist evaluation [QUI08]
- Open Vulnerability and Assessment Language (OVAL) 5.3 and 5.4, a language for representing system configuration information, assessing machine state, and reporting assessment results
- Common Platform Enumeration (CPE) 2.2, a nomenclature and dictionary of hardware, operating systems, and applications [BUT09]
- Common Configuration Enumeration (CCE) 5, a nomenclature and dictionary of security software configurations
- Common Vulnerabilities and Exposures (CVE), a nomenclature and dictionary of security-related software flaws[9]
- Common Vulnerability Scoring System (CVSS) 2.0, an open specification for measuring the relative severity of software flaw vulnerabilities [MEL07].

Section 3 presents detailed information on each of these specifications and provides examples of how these components are used in context.

Security products and checklist authors assemble content from SCAP data repositories to create viable SCAP-expressed security guidance. As stated in the Executive Summary, a security configuration checklist that documents desired security configuration settings, installed patches, and other system security elements using SCAP in a standardized format is known as an SCAP-expressed checklist. Such a checklist would use XCCDF to describe the checklist, CCE to identify security configuration settings to

[7] NIST SP 800-117 is available at http://csrc.nist.gov/publications/PubsSPs.html.
[8] http://nvd.nist.gov/
[9] CVE does not have a version number.

be addressed or assessed, and CPE to identify platforms for which the checklist is valid. The use of CCE and CPE entries within XCCDF checklists is an example of an SCAP convention—a requirement for valid SCAP usage. These conventions are considered part of the definition of SCAP 1.0 and are described in Sections 3, 4 and 5 of this document. Organizations producing SCAP content should adhere to these conventions to ensure the highest degree of interoperability.

SCAP revisions are managed through a coordinated process defined within the SCAP Release Cycle.[10] The release cycle workflow manages changes related to SCAP specifications and validation processes including the addition of new specifications or updates to existing specifications. This process encourages community involvement, promotes transparency and awareness regarding proposed changes, and affords ample lead-time to prepare for pending changes.

[10] SCAP Release Cycle, http://scap.nist.gov/timeline.html

3. Basics of SCAP Components

SCAP 1.0 is comprised of the six specifications referenced in Section 2: XCCDF, OVAL, CPE, CCE, CVE, and CVSS. These specifications are grouped into the following three categories:

- **Languages.** SCAP languages provide a standardized means for identifying what is to be evaluated and for expressing how to check system state.
- **Enumerations.** SCAP enumerations provide a standardized nomenclature (naming format) and an associated dictionary of items expressed using that nomenclature. For example, CVE provides a dictionary of publicly known information security vulnerabilities and exposures.[11]
- **Vulnerability measurement and scoring systems.** SCAP vulnerability measurement and scoring systems provide the ability within SCAP to measure and evaluate specific vulnerability characteristics to derive a vulnerability severity score.

This section provides an introduction to the SCAP component specifications in each of these categories.

3.1 Languages

This section describes the two language specifications in SCAP 1.0: XCCDF 1.1.4 and OVAL 5.3 and 5.4. For each specification, the section describes its purpose and primary logical concepts, and provides examples.

3.1.1 Extensible Configuration Checklist Description Format (XCCDF) 1.1.4

XCCDF 1.1.4 is a specification language for expressing security configuration checklists, vulnerability alerts, and other related documents. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. An XCCDF document represents a structured collection of system review capabilities for some set of target systems. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform means of expressing security checklists and the results of checklist evaluation.

An XCCDF document is composed of one or more XCCDF rules. An XCCDF rule is a high-level definition of a technical check on a system. A rule does not directly specify how a check should be performed, but instead points to other XML documents (such as OVAL Definition files) that contain the actual instructions for performing the check. Table 3-1 shows sample values from an XCCDF rule. This particular rule is for ensuring that the minimum password length is set to at least eight characters. The System Check section of the rule specifies the OVAL Definition example presented in Table 3-3.

[11] http://cve.mitre.org/

Table 3-1. XCCDF Rule Sample Data

Rule Field	Explanation	Sample Data
Rule ID	The identifier for this rule	MinimumPasswordLength-8
Title	The title for the rule	Minimum Password Length = 8
Description	The description of the rule	This setting specifies the minimum length of a password in characters. The rationale behind this setting is that longer passwords are more difficult to guess and crack than shorter passwords. The downside is that longer passwords are often more difficult for users to remember.
References	References to checklists and other documents that contain requirements to which this rule maps—in this case, the IA-5 (Authenticator Management) control from NIST SP 800-53	IA-5 (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf)
Requires	The id of another Group or Rule in the Benchmark that should be selected for this Rule to be applied and scored properly. In this case, the IA-5 group	IA-5
Schema	The XML check system schema to use during rule evaluation (usually the OVAL schema)	http://oval.mitre.org/XMLSchema/oval-definitions-5
OVAL Definition File Reference	Name of the OVAL Definition file	WindowsXP-SP800-68.xml
OVAL Definition ID	The identifier of the OVAL Definition to be used	oval:gov.nist.1:def:20

The number of rules appearing in a typical XCCDF document will vary depending upon the intended use case. The rules appearing in an XCCDF document may also be organized into multiple *XCCDF profiles* that specify collections of rules to be evaluated on particular types of systems. Profiles can be used to express multiple policies within a single benchmark document; allowing the benchmark author to publish technical security control settings tailored to the type of system or the environment in which the system is deployed. By creating a policy that corresponds to a particular set of requirements, such as those of the FISMA, the Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIG), or the Health Insurance Portability and Accountability Act (HIPAA), the policy can be used to map those high-level requirements to the corresponding OVAL Definitions.

An XCCDF document can be further organized into one or more *XCCDF groups*. A group can contain one or more related rules or groups. Groups allow multiple rules to be enabled or disabled collectively instead of individually.

Another option involving XCCDF rules is to have user-definable values for certain rules, known as *XCCDF values*. Table 3-2 shows sample data from an XCCDF value statement. This particular value statement defines the duration of the account lockout (in minutes) that occurs after consecutive failed login attempts have exceeded a specific threshold. In this case, the value has been set to 15 minutes and the operator field specifies that the system setting for lockout duration is greater than or equal to this value. A checklist user may choose to alter or override this value in the profile(s) that reference this value to account for specific organizational policies.

Table 3-2. XCCDF Value Statement Sample Data

Rule Field	Explanation	Sample Data
Value ID	The identifier for this value	AccountLockoutDurationTime
Type	The type of the value (e.g., string, number)	Number
Operator	The comparison operator (in this case, the system's value for account lockout duration time must be greater than or equal to the specified value)	greater than or equal
Title	The title for the value	Account Lockout Duration Time
Description	The description of the value	This value specifies how long the user account should be locked out. This is often set to a low but substantial value (e.g., 15 minutes.
Question	Explanatory text that can be presented to the user when is customizing the checklist	Account lockout duration time (in minutes)
Value	The value assigned to the AccountLockoutDurationTime value	15
Default	A suggested default value number for checklist users' reference; not actually used when performing checks or applying configuration settings	15

3.1.2 Open Vulnerability and Assessment Language (OVAL) 5.3 and 5.4

OVAL is used to express standardized, machine-readable rules that can be used to assess the state of a system. Under SCAP, OVAL is commonly used to determine the presence of vulnerabilities and insecure configurations. A set of instructions used to check for a security problem, such as an incorrect minimum password length setting, is known as an *OVAL Definition*. A file containing one or more OVAL Definitions (often hundreds or even thousands) is known as an *OVAL Definition file*.

There are four types of OVAL Definitions:[12]

- Vulnerability definitions, which define "the conditions that must exist on a computer for a specific vulnerability to be present"
- Patch definitions, which define "the conditions on a computer that determine whether a particular patch is appropriate for a system"
- Inventory definitions, which define "the conditions on a computer that determine whether a specific piece of software is installed on the system"
- Compliance definitions, which define "the conditions on a computer that determine compliance with a specific policy or configuration statement".

Table 3-3 shows sample values that have been extracted from an actual OVAL compliance definition. Explanations of each value have also been provided. The definition ID, version, and class are standard fields that are part of every OVAL Definition. The exact types of information contained in the metadata vary among definitions, but at a high level they explain the intent of the definition. The criteria provide

[12] These definitions are taken from the OVAL Web site's "Structure of the Language" page, located at http://oval.mitre.org/language/about/structure.html.

the technical details of how the system will be checked for the items of interest, such as the presence of a vulnerability or the value of a configuration setting. Each OVAL Definition has a single top-level criterion that can contain one or more sub-criteria. The operator associated with each criterion specifies how the results produced by the sub-criteria are combined (e.g., AND, OR).[13]

The example in Table 3-3 has two criteria. One of the criteria is an *OVAL Test*, which is a specific system check—in this case, that the system is configured to require a minimum password length of at least eight characters. The other criterion is actually another definition—in this case, an inventory definition that confirms that the target system is running Windows XP SP2 on a 32-bit architecture.

Table 3-3. OVAL Definition Sample Data

Definition Field	Explanation	Sample Data
ID	Identifier for this definition; must be globally unique	oval:gov.nist.1:def:20
Version	Version of the definition	1
Class	Defines the type of definition (e.g., compliance, inventory, patch, vulnerability)	Compliance
Metadata		
Title	Short description for the definition	Minimum Password Length of 8 Characters
Affected product	The operating system or application version(s) to which this definition is applicable	Microsoft Windows XP, SP2, 32 bit
References	References to checklists and other documents that contain requirements to which this definition maps	NIST SP800-68 Appendix A, 1.4b, http://csrc.nist.gov/itsec/download_WinXP.html DISA FSO Checklist, 5.4.1.3 DISA VMS 6XID V0001106 DISA PDI ID 1740
Description	Description for the definition	The minimum allowable password length is 8 characters
Criteria		
Definition reference	The identifier of another OVAL Definition, OVAL definition references another OVAL definition (extended definition)	oval:gov.nist.1:def:9
Definition comment	A brief explanation of what the definition addresses; in this case, it is used to determine if the target system is running Windows XP SP2 on a 32-bit architecture	Precondition 9: Windows family, Windows XP, SP2, 32 bit
Test reference	An identifier for an OVAL Test that is run when evaluating the OVAL definition.	oval:gov.nist.1:tst:16
Test comment	A brief explanation of what the test addresses; in this case, it is used to determine if the target system requires a minimum password length of 8 characters	Minimum password length is 8 characters

[13] In the context of this publication, the words ‘criterion’ and ‘criteria’ are used properly; however, the reader should note that the actual OVAL element names are expressed using ‘criteria’ where this document expresses the term ‘criterion’ and ‘criterion’ where this document expresses the term ‘criteria’.

As the example in Table 3-3 shows, definitions often reference one or more tests. The instructions that comprise each test are also included in the OVAL Definition file. A test does not directly contain the technical details of checking the system but instead references other OVAL constructs. Typically, a test references an *OVAL Object*, which is a logical construct for a portion of the target system (e.g., password policy, file, Windows registry key), and an *OVAL State*, which is a particular check of the specified OVAL object (e.g., verifying that the password policy requires a minimum password length of at least eight characters, verifying the existence of a file). An OVAL State can also reference one or more OVAL Variables, which are user-definable values (e.g., minimum password length value of eight). This modular approach introduces additional complexity but fosters reuse and allows OVAL Definitions to be used without requiring the details of test construction to be exposed. Individuals seeking detailed information can refer to the OVAL Definition file for the definition, Test, Object, and State ID numbers, and instructions associated with each entity. More technical details on OVAL Definition files, including examples of the XML code for OVAL Definitions, are presented in Section 4. An OVAL Definition tutorial is also available from the OVAL Web site at http://oval.mitre.org/language/about/definition.html.

3.2 Enumerations

This section describes the three enumeration specifications in SCAP 1.0: CPE 2.2, CCE 5, and CVE. SCAP enumerations typically consist of an identifier, an associated description or definition, and a list of supporting references. For each specification, the section describes its purpose and provides examples of entries. The section also explains the interdependencies between these specifications and other SCAP component specifications.

3.2.1 Common Platform Enumeration (CPE) 2.2

CPE 2.2 is a standard naming convention for operating systems, hardware, and applications. The purpose of CPE is to provide consistent names that can be shared by multiple parties and solutions to refer to the same specific platform type[14].

The syntax of an individual CPE Name, as defined in Section 5 of the CPE 2.2 Specification, is as follows:

```
cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}
```

For example, "`cpe:/o:redhat:enterprise_linux:2.1::es`" refers to Red Hat Enterprise Server 2.1. The "o" indicates that this CPE describes an operating system. In this example, the edition field is blank, indicating that this CPE refers to all editions of Red Hat Enterprise Server 2.1.

CPE Names are used in conjunction with many of the SCAP specifications to provide an association to asset-related information. CPE is used by SCAP in the following ways:

- **XCCDF** – In an XCCDF checklist, CPE Names can be used to identify the hardware or software platform to which an XCCDF object (e.g., benchmark, profile, group, rule) applies.
- **CCE** – CPE Names can be associated with configuration vulnerabilities to identify platforms covered by CCE technical mechanisms.

[14] The MITRE Corporation maintains the CPE specification and NIST maintains the Official CPE Dictionary. More information on CPE is available at http://cpe.mitre.org/. The Official CPE Dictionary is available at http://nvd.nist.gov/cpe.cfm

- **CVE** – CVEs are related to one or more product platforms expressed as CPEs. The mapping of CPEs to CVEs is performed by NVD analysts and is published in the NVD vulnerability data feed.

3.2.2 Common Configuration Enumeration (CCE) 5

The CCE 5 naming scheme is a dictionary of names for security configuration settings for deployed software. Each type of security-related configuration issue is assigned a unique identifier to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. The MITRE Corporation publishes the CCE list.[15]

There are five attributes in a CCE entry: a unique identifier number, a description of the configuration issue, logical parameters of the CCE, the associated technical mechanisms related to the CCE, and references to additional sources of information. Figure 3-1 provides an example of these attributes for a CCE 5 entry for Windows XP:

Figure 3-1. Example CCE Entry

CCE ID:	**CCE-3108-8**
Definition:	**The correct service permissions for the Telnet service should be assigned.**
Parameters:	**(1) set of accounts (2) list of permissions**
Technical Mechanisms:	(1) set via Security Templates (2) defined by Group Policy
References:	Listed at http://cce.mitre.org/lists/cce_list.html

References to CCEs are used by some of the other SCAP specifications to provide an association to particular security configuration settings. In an XCCDF checklist, CCEs can be used to specify which security configuration settings are of interest (i.e., which settings should be checked). Similarly, OVAL uses CCE entries for the same purpose.

3.2.3 Common Vulnerabilities and Exposures (CVE)

CVE is a dictionary of unique, common names for publicly known software flaws[16]. This common naming convention allows sharing of data within and among organizations and enables effective integration of services and tools. For example, a remediation tool may use CVE information from several scanning tools and monitoring sensors, enabling an integrated risk mitigation solution. CVE provides the following:

- A comprehensive list of publicly known software flaws
- A globally unique name to identify each vulnerability
- A basis for discussing priorities and risks of vulnerabilities
- A way for a user of disparate tools and services to integrate vulnerability information

[15] See http://cce.mitre.org/ for additional information.

[16] CVE issuance is managed by The MITRE Corporation and is sponsored by the DHS National Cyber Security Division (NCSD). General CVE information is available at http://cve.mitre.org/.

A CVE vulnerability entry consists of a unique name (e.g., CVE-2000-0001), a short description (e.g., "RealMedia server allows remote attackers to cause a denial of service via a long ramgen request."), and references to public advisories on the vulnerability.

CVE is used in conjunction with other SCAP specifications to satisfy the following use cases:

- **XCCDF.** In an XCCDF checklist, CVEs are used to uniquely identify which software flaw vulnerabilities are of interest (i.e., flaws that are to be checked during the evaluation of the checklist).
- **CVSS.** CVSS scores are associated with CVE entries to uniformly express the fundamental characteristics of the software flaw and to provide a severity score based on these characteristics.
- **OVAL.** Including the specific CVE entry in the OVAL metadata enables a reviewer to accurately understand the basis for a given OVAL definition such as a Vulnerability or Patch test.

Working with researchers, The MITRE Corporation assigns CVE IDs to publicly known vulnerabilities in commercial and open source software.[17]

3.3 Common Vulnerability Scoring System (CVSS) 2.0

CVSS 2.0 provides a repeatable method for consistently evaluating and expressing the risk associated with a given software flaw (e.g., CVE). The use of this shared scoring model allows meaningful comparisons of vulnerability severity scores. CVSS provides three metric groups that can be used to derive a vulnerability score:

- Base, which uses the intrinsic characteristics of the vulnerability to provide a generic score
- Temporal, which captures external factors that may change over time (e.g., availability of exploit code). The base score is adjusted to render a temporal score that accounts for the temporal factors
- Environmental, which characterizes the severity of a vulnerability in the context of an organization's operating environment

The purpose of performing CVSS scoring is to help organizations understand the relative importance of various vulnerabilities so that they can effectively assess, prioritize and mitigate vulnerabilities. Because hundreds of vulnerabilities are publicly announced every week, it is important for organizations to have an easy way to identify those vulnerabilities that have the greatest operational impact. NVD analysts compute and publish CVSS base scores for all CVEs, but organizations are encouraged to further tailor these scores by employing the temporal and environmental metrics to more precisely measure the risk a vulnerability represents within their specific organization.

Complete examples of CVSS measures and scores are available in the official CVSS 2.0 specification [MEL07]. A brief example of base measures, extracted from [MEL07], is [AV:N/AC:L/Au:N/C:C/I:C/A:C], with a base score of 10.0. The bracketed notation for the base measures is known as a *vector*. The first half of the notation indicates that the Access Vector is Network, the Access Complexity is Low, and the Authentication requirement is None. The second half of the notation indicates that the potential impact to Confidentiality, Integrity, and Availability is Complete.

[17] The CVE repository maintained by NIST contains all CVEs issued by The MITRE Corporation as well as supplemental data such as CVSS base scores, vendor statements, and Spanish language translations. NVD provides fine-grained searching and statistical analysis capabilities as well. CVEs and associated NIST-provided metadata can be viewed at http://nvd.nist.gov/nvd.cfm.

The scoring scale is 0 to 10, with 10 being the most severe, so a score of 10.0 indicates the highest severity possible.

The CVSS Special Interest Group from the Forum of Incident Response and Security Teams (FIRST) developed CVSS 2.0. More information on CVSS can be found at http://www.first.org/cvss.

4. SCAP General Requirements and Conventions

As described in NIST Special Publication 800-117, *Guide to Adopting and Using the Security Content Automation Protocol*,[18] the motivation for creating SCAP was to provide a standardized approach to maintaining the security of enterprise systems, enhance interoperability of security products, and enable consistent security assessments. The following conventions and requirements were established to help satisfy these goals by ensuring that validated tools and content interoperate as designed and provide the expected results.

4.1 XCCDF Conventions and Requirements

An SCAP XCCDF document is a machine-readable XML document that defines the policies and test conditions to be evaluated or applied. Types of XCCDF documents include Definition documents that express policy statements and Result documents that contain both policy statements and actual test results.

An SCAP Benchmark document validates against the XCCDF schema (http://scap.nist.gov/specifications/xccdf/) and conforms to all relevant content requirements as outlined in the XCCDF Specification [QUI08].

In cases where localized text is used, US English is the default language. If a `@lang` attribute is omitted, the `@lang` attribute of the nearest ancestor `<xccdf:Benchmark>`, `<xccdf:Value>`, `<xccdf:Group>` and `<xccdf:Rule>` element should be consulted. If this value is omitted, then a value of lang="en-US" SHALL be used by default.

4.1.1 Metadata

XCCDF metadata provides descriptive information about the security benchmark. The metadata is used by SCAP tools to assist in the selection of the appropriate benchmark, ensure that the most recent or correct version of a benchmark is used, and to provide additional information about the benchmark.

The following requirements and conventions apply to the `<xccdf:Benchmark>` element:

> The REQUIRED `@id` attribute SHALL be used to uniquely identify all revisions of a benchmark globally.
>
> The `@style` attribute, if provided, SHALL have the value "SCAP_1.0". If not provided, its value SHALL be assumed to be "SCAP_1.0". **This will be a REQUIRED attribute in SCAP 1.1.**
>
> The `<xccdf:status>` element indicates the current status of the benchmark document. The associated text value MUST be "draft" for documents released in public draft state and "accepted" for documents that have been officially released by an organization. It is RECOMMENDED that the `date` attribute be populated with the date of the status change. Additional `<xccdf:status>` elements MAY be included to indicate historic status transitions.
>
> The `<xccdf:version>` element SHALL uniquely identify the particular revision of the benchmark.

[18] NIST SP 800-117 is available at http://csrc.nist.gov/publications/PubsSPs.html.

One or more instances of the *<xccdf:notice>* element MAY be provided indicating clarifications, suggestions, or warnings regarding the use of the benchmark, including but not limited to terms of use, legal notices or copyright statements.

The *<xccdf:metadata>* element MAY be provided. It is RECOMMENDED that this element contains the following Dublin Core[19] terms: *<dc:creator>*, *<dc:publisher>* and *<dc:contributor>*. **This metadata will be REQUIRED in SCAP 1.1.**

The following requirements and conventions apply to the *<xccdf:Benchmark>*, *<xccdf:Profile>* *<xccdf:Value>*, *<xccdf:Group>* and *<xccdf:Rule>* elements:

One or more instances of the *<xccdf:title>* element SHALL be provided. Each instance MUST contain text values that indicate the purpose of the benchmark delimited by an OPTIONAL *language* attribute. If more than one *<xccdf:title>* element is provided then the language attribute SHALL be provided. An *<xccdf:title>* element SHALL be provided that represents an "en-US" title.

One or more instances of the *<xccdf:description>* element SHALL be provided. Each instance MUST contain text values that represent the purpose and intended audience of the benchmark delimited by an OPTIONAL language attribute. If more than one *<xccdf:description>* element is provided then the language attribute SHALL be provided. An *<xccdf:description>* element SHALL be provided that represents an "en-US" description.

One or more instances of the *<xccdf:reference>* element MAY be included. These elements SHALL provide a cross reference to additional information, preferably including a URL, to obtain additional information regarding the benchmark.

All remaining OPTIONAL elements in the XCCDF schema MAY be included at the author's discretion unless otherwise noted in this document,

For an example, refer to the appendix section D.1 lines 31-35.

4.1.2 XCCDF and CPE Dependencies

For all SCAP content, the applicability of XCCDF *<xccdf:Benchmark>* elements to specific IT platforms SHALL be specified using Common Platform Enumeration (CPE) Names.

CPE Names used within an XCCDF benchmark SHALL match the names of existing Official CPE Dictionary[20] entries where possible. If multiple matches are found within the dictionary (e.g., deprecated and current CPE Names), the most current CPE Name SHOULD be used.

Each *<xccdf:Benchmark>* bound to a CPE Name SHALL be declared in the required CPE dictionary stream and each OVAL inventory class definition referenced from the dictionary stream SHALL be specified in the required CPE inventory stream.

Use of CPEs bound to *<xccdf:Profile>*, *<xccdf:Group>*, and *<xccdf:Rule>* elements SHALL NOT be allowed.

---

[19] http://dublincore.org/documents/dces/

[20] The Official CPE Dictionary is located at http://nvd.nist.gov/cpe.cfm.

4.1.3 <Rule> Element

The following requirements and conventions apply to the *<xccdf:Rule>* element:

> When defining the *@id* attribute it is important to take into consideration the long-term use of the Rule. As most Rule identifiers are generated by humans today, there is a tendency to encode meaning in the identifier. This can create contradictions within the @id attribute relative to the containing document or policy as content is re-used and re-purposed. It is RECOMMENDED that information is omitted in the identifier that references: the target platform, assessed values, and/or security guide context.
>
> The *@weight* attribute SHALL be provided on *<xccdf:Rule>* elements. The value for this element SHALL be defined as "10.0" as a placeholder for Common Configuration Scoring System (CCSS) scores to indicate the highest possible weight. Once the CCSS is adopted into a future version of SCAP and CCSS scores are available, these values will be replaced with appropriate CCSS scores.
>
> If the XCCDF document represents software flaws, then the CVSS metric SHALL be defined in the *@weight* attribute on the *<xccdf:Rule>* elements.

4.1.4 Embedded CCE References

XCCDF *<xccdf:Rule>* elements MAY be used to define a policy requiring compliance with a specific configuration setting. When a configuration setting having one or more associated CCE Identifiers from the CCE List is expressed as an XCCDF rule, an *<xccdf:ident>* element[21] reference SHALL be provided within the *<Rule>* element. The *<xccdf:ident>* element provides a globally unique identifier for a specific configuration setting.

The *<xccdf:ident>* element syntax SHALL be used as follows:

1. The system attribute for the *<xccdf:ident>* element SHALL be defined using the CCE Version 5 system identifier "*http://cce.mitre.org*".
2. The *CCE Identifier* SHALL be used for the *<xccdf:ident>* element content.

For example:

```
<Rule id="AuditAccountLogonEvents">
    <title>Audit Account Logon Events</title>
    …
    <ident system="http://cce.mitre.org">CCE-3867-0</ident>
    <ident system="http://cce.mitre.org">CCE-3008-0</ident>
    …
</Rule>
```

A rule result of "pass" indicates that the target platform complies with the configuration setting guidance expressed in the XCCDF rule.

[21] See NIST IR 7275r3, The XCCDF Specification version 1.1.4, p.21 table, p.22 paragraph 5, and p.59 section "<ident>" for additional details.

4.1.5 Embedded CVE References

XCCDF *<xccdf:Rule>* elements MAY be used to assess security related software flaws. When this assessment is associated with one or more associated CVE Identifiers from the CVE vulnerability feeds, an *<xccdf:ident>* element[22] reference within the *<xccdf:Rule>* element SHALL be provided.

The *<xccdf:ident>* element syntax SHALL be used as follows:

1. The system attribute for the *<xccdf:ident>* element SHALL be defined using the CVE system identifier "*http://cve.mitre.org*".
2. The *CVE Identifier* SHALL be used for the *<xccdf:ident>* element content.

For example:

```
<Rule id="SQLInjectionVulnerability"
    <title>SQL Injection Vulnerability</title>
    …
    <ident system="http://cve.mitre.org">CVE-2008-6865</ident>
    <ident system="http://cve.mitre.org">CVE-2008-6866</ident>
    …
</Rule>
```

A rule result of "pass" indicates that the target platform satisfies all the conditions of the XCCDF rule and is unaffected by the vulnerability or exposure referenced by the CVE.

4.1.6 Allowed Check System Usage

The following requirements and conventions apply to the use of the *<xccdf:check>* element and check systems in general.

The *<xccdf:complex-check>* element SHALL NOT be used.

The *<xccdf:check-content>* element SHALL NOT be used to embed check content directly into XCCDF content.

If multiple *<xccdf:check-content-ref>* elements are provided, then processing SHALL:

1. Evaluate each *<xccdf:check-content-ref>* element in the order that it appears in the *<xccdf:check>* element. The first resolvable *<xccdf:check-content-ref>* element SHALL be used to determine the *<xccdf:Rule>* status.
2. For each *<xccdf:check-content-ref>* element, a tool will attempt to retrieve the document referenced by the *@href* attribute. If not resolvable, the next available *<xccdf:check-content-ref>* element SHALL be evaluated. If none of the *<xccdf:check-content-ref>* elements are resolvable, then the result of the rule evaluation SHALL be the XCCDF "error" status and processing of the *<xccdf:Rule>* SHALL end. Please note that it is acceptable to map a remote URL to a local copy of the file in cases where remote access is not available, not allowed or not practical.
3. Once a resolvable *<xccdf:check-content-ref>* element is found, then check system processing SHALL proceed.

For example, refer to the appendix section D.1 lines 223-226.

[22] See NIST IR 7275r3, The XCCDF Specification version 1.1.4, p.21 table, p.22 paragraph 5, and p.59 section "<ident>" for additional details.

4.1.7 Use of the OVAL as a Check System

A rule MAY refer to one or more OVAL Definitions to implement the technical tests necessary to determine the pass/fail status of the rule. Embedded OVAL Definitions are not supported by SCAP XCCDF. References from SCAP compliant XCCDF to OVAL Definitions SHALL use the form:

```
<check-content-ref href="OVAL_Source_URI" [name="OVAL_Definition_Id"]/>
```

The `href` attribute identifies the OVAL Definition XML stream. When present, the optional `name` attribute refers to a specific OVAL definition in the designated content stream. When an XCCDF rule references a specific OVAL Definition, an OVAL Definitions source SHALL be available to resolve the reference.

SCAP stylistic conventions specify that the optional `name` attribute be omitted if the rule is designed to evaluate the current patch level of the target platform. The following rule specification is an example of this convention:

```
<Rule id="SecurityPatchesUpToDate" selected="false" weight="10.0">
      <title>Security Patches Up-To-Date</title>
      <description>Keep systems up to current patch levels</description>
      <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
            <check-content-ref href="scap-win2000-patches.xml"/>
      </check>
</Rule>
```

In the previous example, the *<xccdf:check-content-ref>* element's *href* attribute refers to an OVAL Definitions stream containing one or more OVAL patch definitions. This *check-content-ref* is equivalent to *referencing* a virtual OVAL Definition of the form:

```
<oval_definitions xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5">
 <definitions>
      <definition id="identifier of patch definition" version="0" class="patch">
        …
        <criteria >
         <extend_definition definition_ref="identifier of patch definition 1"/>
         …
         <extend_definition definition_ref="identifier of patch definition N"/>
        </criteria>
    </definition>
</oval_definitions>
```

where the extended definitions are the individual patch definitions defined in the OVAL content stream.[23]

If any *<xccdf:Rule>* references an OVAL patch definition, a patch scan source SHALL be used to resolve the reference.

[23] The Inventory definition results are not to be considered in the overall patch results. The intent is to logically combine the result of each definition with a class of 'patch' using the AND operation. The patch definition file may contain a mix of patch and inventory definitions and the overall patch checking result should be the AND of just the patch definition results values.

4.1.8 *<xccdf:Value>* and OVAL Variable Dependencies

Content authors SHOULD refrain from hard coding assessment values into the OVAL Definitions to maximize the flexibility and reuse of OVAL modules. The recommended approach is to define these values as XCCDF value parameters. An acceptable alternative is to represent these values as discrete OVAL Variables or within an OVAL Variables file.

When the OVAL Definition(s) referenced from a rule require one or more external variable bindings, the check-export element(s) that define the binding of XCCDF values to OVAL variables SHALL precede the check-content-ref element. The format of these elements is:

```
<check-export xmlns=http://checklists.nist.gov/xccdf/1.1
      value-id="XCCDF_Value_id" export-name="OVAL_External_Variable_id"/>
```

The following check element example demonstrates the use of this convention:

```
<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
      <check-export export-name="oval:gov.nist.fdcc.xp:var:66711"
      value id="NoSlowLink_var"/>
      <check-export export-name="oval:gov.nist.fdcc.xp:var:66712"
      value-id="NoBackgroundPolicy_var"/>
      <check-export export-name="oval:gov.nist.fdcc.xp:var:66713"
      value-id="NoGPOListChanges_var"/>
      <check-content-ref href="fdcc-winxp-oval.xml" name="oval:gov.nist.fdcc.xp:def:6671"/>
</check>
```

The type and value binding of the specified XCCDF Value is constrained to match that lexical representation of the indicated OVAL Variable Data Type. Table 4-1 summarizes the constraints regarding data type usage. Additional information regarding OVAL and XCCDF data types can be found in the OVAL Common Schema documentation[24] and the XCCDF specification[25].

Table 4-1. XCCDF-OVAL Data Export Matching Constraints

OVAL Data Type	Matching XCCDF Data Type
Int	number
Float	number
Boolean	boolean
string, evr_string, version, ios_version, fileset_revision, binary	string

4.1.9 XCCDF Test Results

XCCDF test results are documented as the contents of an *<xccdf:TestResult>* element that either stands alone as the root of an XML document or is embedded as a child-element of an *<xccdf:Benchmark>* root element. In the latter case, the associated benchmark is the embedding benchmark; in the former, the *<xccdf:TestResults>* document requires an embedded

[24] http://oval.mitre.org/language/download/schema/version5.4/ovaldefinition/documentation/oval-common-schema.html#DatatypeEnumeration and http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/documentation/oval-definitions-schema.pdf

[25] http://csrc.nist.gov/publications/nistir/ir7275r3/NISTIR-7275r3.pdf

<xccdf:Benchmark> element that identifies the associated benchmark. *<xccdf:Benchmark>* elements are ignored in *<xccdf:TestResult>* elements that are embedded in their associated benchmark.

To be considered valid SCAP content, the following conditions SHALL be met:

- When using a profile during the processing of XCCDF content, the test results SHALL embed an *<xccdf:Profile>* element that identifies the non-abstract profile in the associated benchmark whose evaluation results are reported by the test results.
- Reported rule results SHALL include all selected rules within the specified Profile.
- Reported value-settings SHALL include all those values that are exported by the reported rules. The specific settings are those determined by the reported Profile.
- The *<identity>* tag identifies the security principal used to access rule evaluation on the target(s).
- The *<rule-result>* elements SHALL report the result of the application of each selected rule against all specified targets. The *rule_idref* attribute of the *<xccdf:rule-result>* SHALL identify the selected rule and each *<xccdf:instance>* element SHALL identify the corresponding *<xccdf:target>* element.

4.1.10 Assigning CVE Identifiers to Rule Results

The XCCDF *<xccdf:rule-result>* element provides data indicating the result of assessing a system using the identified XCCDF *<xccdf:Rule>* element. If the target XCCDF *<xccdf:Rule>* identified by the <xccdf:*rule-result idref=””>* attribute has one or more *<ident>* elements[26] with the "*http://cve.mitre.org"* system identifier, then each *<xccdf:ident>* element SHOULD also appear within the *<xccdf:rule-result>* element.

For example:

```
<rule-result idref="minimum_password_length"
      xmlns="http://checklists.nist.gov/xccdf/1.1">
      …
      <cdf:Rule id="java-upgrade-278" selected="1" weight="0.5">
      <cdf:title>Java Bug Fix Upgrade Installed</cdf:title>
      <cdf:ident system="http://cve.mitre.org/> CVE-2006-0614 </cdf:ident>
      …
</rule-result>
```

[26] See NIST IR 7275r3, The XCCDF Specification version 1.1.4, p.30 table and p.59 section "<ident>".

4.1.11 Assigning CCE Identifiers to Rule Results

The XCCDF *<xccdf:rule-result>* element provides data indicating the result of assessing a system using the identified XCCDF <xccdf:Rule> element. If the target XCCDF *<xccdf:Rule>* identified by the <xccdf:*rule-result idref=""*> attribute has one or more *<xccdf:ident>* elements with the "*http://cce.mitre.org"* system identifier, then each *<xccdf:ident>* element SHOULD also appear within the *<rule-result>* element. For example:

```
<rule-result idref="minimum_password_length"
      xmlns="http://checklists.nist.gov/xccdf/1.1">
      …
      <ident system="http://cce.mitre.org">CCE-2981-9</ident>
      …
</rule-result>
```

4.1.12 Mapping OVAL Results to XCCDF Results

When an *<xccdf:Rule>* element references an OVAL Definition, the *<xccdf:rule-result>* that results from the application of that rule specifies an XCCDF rule result that is mapped from the OVAL Definition Result. This result is calculated by applying the referenced OVAL Definition to a target platform.

In some cases the derived results may seem counterintuitive, but when viewed in the appropriate context the underlying logic is evident. For example, if an OVAL Definition of class "compliance" is processed and the XCCDF returns a result of "True", the tool is conveying the fact that the system was found to be compliant with that check and therefore returns a "Pass" result. A similar definition for a vulnerable condition will return results of "False" if that vulnerability was not found on the examined devices, resulting in a "Pass" from the XCCDF rule. SCAP compliant processors that generate XCCDF rule results SHALL apply the mapping illustrated in Table 4-2 when deriving XCCDF rule results from OVAL definition results.

SCAP users may reference several classes of OVAL Definitions from a single XCCDF document (e.g., a single SCAP-expressed checklist that performs configuration verification AND patch compliance checks.) Users of multiple OVAL Definition classes must consider the effect of the definition class when interpreting definition results and ensure that rule evaluation produces the correct results.

Table 4-2. Deriving XCCDF Rule Results from OVAL Definition Results

<table>
<tr><th colspan="2">OVAL Definition Result</th><th>XCCDF Rule Result</th></tr>
<tr><td colspan="2">Error</td><td>Error</td></tr>
<tr><td colspan="2">Unknown</td><td>Unknown</td></tr>
<tr><td colspan="2">Not applicable</td><td>Notapplicable</td></tr>
<tr><td colspan="2">Not evaluated</td><td>Notchecked</td></tr>
<tr><td>Definition Class</td><td>Definition Result</td><td rowspan="5">Pass</td></tr>
<tr><td>Compliance</td><td>True</td></tr>
<tr><td>Vulnerability</td><td>False</td></tr>
<tr><td>Inventory</td><td>True</td></tr>
<tr><td>Patch</td><td>False</td></tr>
<tr><td>Definition Class</td><td>Definition Result</td><td rowspan="5">Fail</td></tr>
<tr><td>Compliance</td><td>False</td></tr>
<tr><td>Vulnerability</td><td>True</td></tr>
<tr><td>Inventory</td><td>False</td></tr>
<tr><td>Patch</td><td>True</td></tr>
</table>

4.2 OVAL Conventions and Requirements

When used for SCAP purposes, OVAL content SHALL comply with one of the following document schema:

- *<oval-def:oval_definitions>* document – A specification of OVAL Definitions, Tests, Objects, States and Variables. This document may optionally be used as a component of an SCAP data source.
- *<oval-var:oval_variables>* document – A specification of external OVAL Variable bindings. This document may optionally be used as a component of an SCAP data source.
- *<oval-sc:oval_system_characteristics>* document – A specification of target system characteristics, that is, the specification of OVAL Object values queried from a target system
- *<oval-res:oval_results>* document – The evaluation results of specified definitions and tests, as well as a copy of the OVAL System Characteristics from which the results can be derived.

4.2.1 OVAL Schema Specification

All of the OVAL content MUST contain an *<oval:generator>* element**.** The bundle version of any particular document instance SHALL be specified using the *<oval:schema_version>* content element of the *<oval:generator>* as in this example:

```
<oval:generator>
  <oval:product_name>The OVAL Repository</oval:product_name>
  <oval:schema_version>5.3</oval:schema_version>
</oval:generator>
```

The bundle version of an *<oval-def:oval_definitions>* document SHOULD be chosen based on the version provided in the *<oval:generator>/<oval:schema_version>* element's value.

The bundle version of an *<oval-var:oval_variables>* document SHALL be the same as that of the *<ovaldef:oval_definitions>* document whose external variables are bound by the variables document.

Production of *<oval-sc:oval_system_characteristics>* or *<oval-res:oval_results>* is OPTIONAL. If an *<oval-sc:oval_system_characteristics>* or *<oval-res:oval_results>* document is generated as a consequence of the application of a *<oval-def:oval_definitions>* ***document***, then the bundle version of the generated document SHALL be the same as that of the *<oval-def:oval_definitions>* ***document***.

4.2.2 OVAL Definitions and Affected Platforms

The *<oval-def:metadata>* element of an *<oval-def:definition>* optionally identifies platforms affected by including *<oval-def:affected>* elements. One or more of these elements SHALL be present whenever the class of the *<oval-def:definition>* is "vulnerability",

"compliance", "patch", or "inventory".[27] `<oval-def:affected>` elements MAY be used when the definition class is "miscellaneous". If more than one `<oval-def:affected>` element is included in definition metadata, then the family attribute of each of the `<oval-def:affected>` elements SHALL be bound to the same value[28]. Thus each `<oval-def:definition>` is either associated with a single family, or the family association of the definition is undefined (only allowed for OVAL definitions whose class is "miscellaneous").

If the family association of an OVAL Definition is undefined, any definitions extended by that definition SHALL also have undefined family associations. If the family association of an OVAL Definition is specified, then any definitions extended by that definition SHALL be the same as that of the extending definition or SHALL have an undefined family association.

For the purposes of SCAP, an OVAL Definition's family association also determines the kinds of tests that it can reference as `<oval-def:criterion>`. Table 4-3 maps the family associations to the test component schema[29] allowed for the family. Each component namespace is designated by its fractional part; for example, #windows refers to the component namespace URI http://oval.mitre.org/XMLSchema/oval-definitions-5#windows.

Table 4-3. Association of Family to Component Schemas

Family	Allowed Subschemas
undefined	#independent
ios	#independent #ios
macos	#independent #macos
unix	#independent #hpux #linux #solaris #unix
windows	#independent #windows

4.2.3 OVAL Definitions and Compliance Validation

An OVAL compliance Definition is an `<oval-def:oval_definitions>` document that specifies definitions for validating the compliance status of target platforms. An OVAL compliance definition SHALL specify at least one definition of class "compliance." An OVAL compliance definition may also reference definitions of class "inventory" that are extended (transitive) by the "compliance" class definitions.

---

[27] The OVAL Definition Schema is available at http://oval.mitre.org/language/download/schema/version5.4/ovaldefinition/documentation/oval-common-schema.html and http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/documentation/oval-definitions-schema.pdf.

[28] The supported family values are "ios", "macos", "unix" and "windows". (http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/documentation/oval-common-schema.pdf).

[29] The OVAL 5.3 test subschema namespaces are:

- http://oval.mitre.org/XMLSchema/oval-definitions-5#independent Supports any OS
- http://oval.mitre.org/XMLSchema/oval-definitions-5#ios Supports Cisco IOS
- http://oval.mitre.org/XMLSchema/oval-definitions-5#hpux Supports HP-UX
- http://oval.mitre.org/XMLSchema/oval-definitions-5#unix Supports Unix dialects
- http://oval.mitre.org/XMLSchema/oval-definitions-5#linux Supports Linux
- http://oval.mitre.org/XMLSchema/oval-definitions-5#macos Supports Apple Macintosh
- http://oval.mitre.org/XMLSchema/oval-definitions-5#solaris Supports Sun Solaris
- http://oval.mitre.org/XMLSchema/oval-definitions-5#windows Supports Microsoft Windows
- http://oval.mitre.org/XMLSchema/oval-definitions-5#freebsd Supports FreeBSD
- http://oval.mitre.org/XMLSchema/oval-definitions-5#apache Supports Apache applications

Refer to http://oval.mitre.org/language/download/schema/version5.3/index.html.

If an OVAL "compliance" class definition maps to one or more CCE identifiers, the definition SHOULD include *<oval-def:reference>* elements that reference those identifiers using the following format:

```
<oval-def:reference source="CCE" ref_id="CCE_identifier"/>
```

4.2.4 OVAL Definitions and Vulnerability Assessment

An OVAL vulnerability definition is an *<oval-def:oval_definitions>* document that specifies definitions for assessing the vulnerability status of target platforms. An OVAL vulnerability definition SHALL specify at least one definition of class "vulnerability" or "patch". An OVAL vulnerability definition may also reference definitions of class "inventory" or "compliance" that are extended (transitive) by the "vulnerability" class definitions.

If an OVAL "patch" or "vulnerability" class definition maps to one or more CVE identifiers, the definition SHOULD include *<oval-def:reference>* elements that reference those identifiers using the following format:

```
<oval-def:reference source="CVE" ref_id="CVE_identifier"/>
```

OVAL "patch" class definitions SHOULD also reference source patch identifiers, if they exist.

4.2.5 OVAL Definitions and Patch Assessment

An OVAL patch definition is an *<oval-def:oval_definitions>* document that specifies definitions for assessing the patch status of target platforms. An OVAL patch definition SHALL specify at least one definition of class "patch". An OVAL patch definition may also include definitions of class "inventory" that are extended (transitive) by the "patch" class definitions.

If an OVAL "patch" class definition is associated with a source specific identifier (for example, KB numbers for Microsoft patches), these identifiers SHOULD be included in *<oval-def:reference>* elements contained by the definition. For example:

```
<oval-def:reference source="www.microsoft.com/Patch" ref_id="KB912919"/>
```

If an OVAL "patch" class definition maps to one or more CVE identifiers, the definition MAY include *<oval-def:reference>* elements that reference those identifiers using the following format:

```
<oval-def:reference source="CVE" ref_id="CVE_identifier"/>
```

4.2.6 OVAL Inventories

An OVAL Inventory component is an *<oval-def:oval_definitions>* document that specifies only "inventory" class definitions for verifying CPE match conditions.

4.2.7 OVAL Results

While the OVAL specification permits limited result status reporting, SCAP-compliant content includes full status reporting including Error, Unknown, Not Applicable, Not Evaluated, True, and False. Section 4.1.12 provides additional detail about OVAL results.

Results returned SHALL be compliant with the OVAL results schema.[30] In order to support SCAP instances where OVAL thin content (only the ID of the definition and the results) is preferred, SCAP content SHALL support all valid values for the ContentEnumeration directives controlling the expected content of the results file. Specific product requirements may be implemented through the Derived Test Requirements.

4.3 CPE Conventions

CPE Names supported by the Official CPE Dictionary data feed or the custodial list supported by The MITRE Corporation[31] may be used by SCAP components to reference CPE Names. The process for assigning new CPE Names is supported by The MITRE Corporation.[32] Local enumerations are permitted, but if a CPE Name for a product or platform exists in the Official CPE Dictionary, the tool SHALL use that official identifier.

Section 8 of CPE Specification 2.2 provides the defining structure of the Official CPE Dictionary. For certain names, a *<cpe_dict:cpe-item>* MAY contain one or more *<check>* elements that reference OVAL system inventory definitions using the following format:

```
<cpe_dict:check system="http://oval.mitre.org/XMLSchema/oval-definitions-5"
      href="Oval_URL">Oval_inventory_definition_id</cpe_dict:check>
```

For example:

```
<cpe-list xmlns="http://cpe.mitre.org/dictionary/2.0"
          xmlns:cpe_dict="http://cpe.mitre.org/dictionary/2.0">

     <cpe-item name="cpe:/o:microsoft:windows_2003">
          <title>Microsoft Windows Server 2003</title>
          <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
                          oval:org.mitre.oval:def:128
          </check>
      </cpe-item>
</cpe-list>
```

The referenced OVAL inventory definition specifies the technical procedure for determining whether or not a specific target asset is an instance of the CPE Name specified by the *<cpe_dict:cpe-item>* element. This usage is encouraged for CPE dictionary components of SCAP expressed data streams.

If a *<cpe_dict:cpe-item>* contained in a CPE dictionary component of an SCAP data stream references an OVAL "inventory" definition, then that definition SHALL be resolved by a CPE Inventory component in the same data stream.[33] Furthermore, the title of the *<cpe_dict:cpe-item>* SHALL match the title of an affected platform bound to the referenced definition.[34]

4.4 CCE Conventions

CCE identifiers are used by SCAP components to reference Common Configuration Enumerations. CCE identifiers for new configuration settings are assigned by the CCE Content Team.[35] To maintain

---

30 The OVAL schemas are described in detail at http://oval.mitre.org/language/about.
31 The Official CPE Dictionary is located at http://nvd.nist.gov/cpe.cfm.
32 Ibid.
33 More information is provided in Section 4.7.
34 Section 4.2.2 explains more detail about OVAL definitions.
35 http://cce.mitre.org/lists/creation_process.html documents the CCE Creation Process.

consistency and accuracy among the SCAP validated tools, if a CCE entry for a particular configuration setting exists in the Official CCE Dictionary, the security products SHALL use the official CCE identifier. If no CCE exists for the configuration setting of interest, an alternate identifier MAY be used, but the user SHOULD seek to have a CCE identifier issued for the vulnerability.

The MITRE Corporation maintains the current official CCE list at http://cce.mitre.org/lists/cce_list.html and new CCEs can be requested from The MITRE Corporation at http://cce.mitre.org/lists/creation_process.html.

4.5 CVE Conventions

CVE identifiers are used by SCAP components to reference publicly known software flaws.[36] CVE references in SCAP content MAY include both "candidate" and "entry" status identifiers. If a CVE identifier exists for a particular vulnerability, security products SHALL use the official CVE identifier. If no CVE exists for the software flaw, an alternate identifier MAY be used, but the user SHOULD seek to have a CVE identifier issued for the vulnerability. The process for submitting unpublished vulnerabilities and obtain CVE identifiers is available from The MITRE Corporation via http://cve.mitre.org/cve/obtain_id.html.

It should be noted that not all CVE entries identify an associated patch or remediation; in fact, the ability to determine the availability of a patch or remediation is a valuable feature of the CVE component. Vendors SHOULD reference CVE entries in notifications (e.g., security patch bulletins) to support the use of automated tools and to ensure clarity when referencing a given vulnerability. Similarly, CVE authors SHOULD reference applicable vendor patch identification whenever possible.

NIST provides a CVE data feed to support dynamic and current vulnerability information and associated metadata (e.g., CVSS values). The current schema is available at http://nvd.nist.gov/download.cfm.

4.6 CVSS Conventions

The CVSS specification (described at http://www.first.org/cvss/cvss-guide.html) defines Base score metrics that characterize the severity of the vulnerability using the intrinsic characteristics of the vulnerability. The CVSS framework also allows further refinement of the base score using Temporal Metrics, which may change over time (e.g., Exploitability, Report Confidence) and Environmental Metrics, which are unique to a particular environment (e.g., Collateral Damage Potential, Target Distribution).

If an accompanying CVSS score exists for a CVE, products SHOULD use it. CVSS base scores are provided for all CVE identifiers contained in the NVD CVE data feed. If a CVSS Base Metric is provided, it SHALL reflect the current Base score as reflected in the official source. SCAP users MAY leverage the flexibility provided within the CVSS component specification by deriving and using the Temporal and Environmental metrics as needed.

[36] NIST provides the NVD CVE data feed at http://nvd.nist.gov/download.cfm#CVE_FEED.

5. SCAP Use Case Requirements

To facilitate implementation of the SCAP requirements specified in Section 4, this section describes specific uses that demonstrate effective use of the protocol. The content of this section identifies the input data source conventions identified with the SCAP components and associates these with the following use case examples:

- Configuration Verification
- Vulnerability Assessment
- Patch Validation
- Inventory Collection

These examples are not intended to limit SCAP but provide a framework for future use cases and document the specifics of the data streams described. SCAP enables many types of automated assessment, each with discrete benefits and each considered separate content. For example, vulnerability assessment (i.e., quantitative and repeatable measurement and scoring of software flaw vulnerabilities across systems) is related to but separate from configuration verification.

An SCAP data stream is the expression of a security use case using one or more SCAP components that can be processed by an SCAP-validated product. The required XML content composing an SCAP data stream depends on the use case and is designed to satisfy specific policy or situational awareness objectives. Every SCAP data stream bundle SHALL use a common locator prefix that is part of a relative URL whose base is the URL of the deployed data source. The notation '*xxxx*' designates a locator prefix that SHALL be associated with a use case specific data source component stream.

For example:

```
file:///c:/content/example-winxp-xccdf.xml

The URL base is: file:///c:/content/
The locator prefix is: example-winxp
The component stream is: xccdf.xml
```

5.1 SCAP Configuration Verification with XCCDF and OVAL

SCAP enables automated processes to compare system characteristics and settings against an SCAP-expressed checklist. Using such a process, such as that referenced in NIST SP 800-68, *Guide to Securing Microsoft Windows XP Systems for IT Professionals*, a user may confirm compliance and identify deviations from checklists appropriate for relevant operating systems and/or applications.

The following data sources are necessary to support SCAP-compliant configuration verification use cases:

Table 5-1. SCAP Configuration Verification Data Sources

Component	Stream Locator	Required/Optional
XCCDF Benchmark	xxxxxccdf.xml	Required
OVAL Compliance	xxxxoval.xml	Required
OVAL Patch	xxxxpatches.xml	Optional
CPE Dictionary	xxxxcpe-dictionary.xml	Required
CPE Inventory	xxxxcpe-oval.xml	Required

For an SCAP configuration verification data source to be processed by the appropriate SCAP-validated product:

- Each Rule specified in the XCCDF benchmark SHALL include an *<ident>* element containing a CCE reference, where an appropriate reference exists.
- If an *<ident>* is specified in an XCCDF benchmark Rule, then that reference SHALL match the CCE reference found in the associated OVAL definition(s).
- The XCCDF *<xccdf:Benchmark>* element SHALL contain references to one or more CPEs.
- A rule bound to a specific CCE may be associated with one or more of the controls described in NIST SP 800-53. The mapping to these controls may be represented in the XCCDF benchmark by applying the following conventions:
  - Use of an official, dynamic data feed is preferred to static coding of values in SCAP data sources. The NVD provides a data feed[37] that correlates CCE identifiers with the control identifiers described in SP 800-53.
  - The SP 800-53 controls referenced within an XCCDF benchmark are represented by *<xccdf:Group>* elements. Note that the XCCDF control group identifiers correspond to the control identifiers found in Appendix F of SP 800-53.
  - Each *<xccdf:Rule>* SHALL be associated with one or more SP 800-53 controls by capturing the ID of the each associated control in an *<xccdf:requires>* element within the rule. This association allows rules to be enabled/disabled at the profile level through the selection/deselection of the associated control groups.
  - The chosen convention for mapping XCCDF rules to SP 800-53 controls within a benchmark SHOULD be uniformly applied to all rules having SP 800-53 mappings.
- XCCDF configuration scanning processes SHALL produce XCCDF Results and OVAL Results that comply with the XCCDF and OVAL Results schema.
- XCCDF Results documents SHALL include a result for each rule that was evaluated during the scan. OVAL Results documents SHALL include the results of every OVAL definition used to generate the reported rule results.
- If an XCCDF rule references a specific OVAL definition, the definition MUST be a compliance class definition.
- An XCCDF benchmark MAY include a "patches up-to-date" rule that references an OVAL patch component stream. If such a rule is used, the OVAL patch component MUST be included in the OVAL compliance data source.
- An XCCDF benchmark MAY enumerate one patch per rule. If this approach is used, a specific OVAL definition of class "patch" MUST be referenced in the OVAL Patch component stream.

5.2 SCAP Vulnerability Assessment

In the context of SCAP, a vulnerability is defined as a software flaw, bug, or defect that introduces a security exposure. SCAP enables interoperability among vulnerability scanners and reporting tools to provide consistent detection and reporting of these flaws and supports comprehensive remediation tool

[37] http://web.nvd.nist.gov/view/ncp/checklist-cce-feed?id=113&cid=2

capabilities. Section 4.1.12 documents the reasons that vulnerability assessment and configuration verification are significantly different use cases, and shows how SCAP results are interpreted under these two use cases.

5.2.1 SCAP Vulnerability Assessment Using XCCDF and OVAL

Effective vulnerability assessment using a combination of SCAP components requires the following data sources:

Table 5-2. SCAP Vulnerability Assessment Data Sources

Component	Stream Locator	Required/Optional
XCCDF Benchmark	xxxxxccdf.xml	Required
OVAL Vulnerability	xxxxoval.xml	Required
OVAL Patch	xxxxpatches.xml	Optional
CPE Dictionary	xxxxcpe-dictionary.xml	Required
CPE Inventory	xxxxcpe-oval.xml	Required

For an SCAP Vulnerability Assessment to be performed by the appropriate SCAP-validated product, the following conditions SHALL be met:

- The XCCDF `<xccdf:Benchmark>` element SHALL contain references to one or more CPEs.
- XCCDF Vulnerability Scanning SHALL generate an XCCDF Results file. The XCCDF Results document SHALL include a result for each rule that was evaluated during the scan.
- Each Rule specified in an XCCDF benchmark SHALL include an `<ident>` element containing a CVE reference, where an appropriate reference exists.
- Each Rule specified in an XCCDF benchmark SHALL reference a specific OVAL vulnerability, patch, or inventory definition; except in cases where no automated mechanism exists to express a check in OVAL.
- If OVAL Results are generated:
  - OVAL Results SHALL be expressed in compliance with the OVAL Results schema, and
  - OVAL Results documents SHALL include the results of every OVAL definition used to generate the reported rule results.
- If a CVE reference is specified in an XCCDF benchmark rule, then that reference SHALL match the CVE reference found in the associated OVAL definition(s).

5.2.2 SCAP Vulnerability Assessment Using Standalone OVAL

For an OVAL-only vulnerability assessment to be processed by the appropriate SCAP-validated product, the following SHALL be present:

- A Standalone OVAL Vulnerability Data Stream SHALL include an OVAL Vulnerability XML stream component that defines the applied OVAL vulnerability class definitions.
- OVAL Definitions SHALL include CVE references, if such exist.

- OVAL vulnerability data scanning SHALL generate an OVAL Results document that complies with the OVAL Results schema and includes the results of every OVAL definition used to generate the reported rule results.
- The OVAL Results document SHALL include a definition result with supporting system-characteristics data for every definition in the vulnerability data source.

5.3 Inventory Collection

Organizations require a consistent protocol for integrating inventory information from among a broad range of products, and SCAP provides excellent methods for collecting this data. For example, SCAP inventory data is an important input to the Risk Management Framework,[38] establishing an effective foundation for system categorization and baseline security controls. For SCAP tools to collect this inventory information, the following data sources are required:

Table 5-3. SCAP Inventory Collection

Component	Stream Locator	Required/Optional
XCCDF Benchmark	xxxxxccdf.xml	Optional
CPE Dictionary	xxxxcpe-dictionary.xml	Required
CPE Inventory	xxxxcpe-oval.xml	Required

In order for an Inventory scan to be processed by the appropriate SCAP-validated product:

- The inventory data source SHALL include an OVAL Inventory component that defines the applied OVAL inventory class definitions.
- OVAL vulnerability data scanning SHALL generate an OVAL Results document that complies with the OVAL Results schema and includes the results of every OVAL definition used to generate the reported rule results.
- The results document SHALL include a definition result with supporting system-characteristics data for every definition in the Inventory component.

[38] The Risk Management Framework is explained in NIST SP 800-53 Revision 3 at http://csrc.nist.gov/publications/PubsSPs.html.

Appendix A— Acronyms and Abbreviations

Appendix A defines selected acronyms and abbreviations used in the document.

CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
FDCC	Federal Desktop Core Configuration
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FSO	DISA Field Security Operations
GPO	Group Policy Object
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
ITL	Information Technology Laboratory
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NSA	National Security Agency
NVD	National Vulnerability Database
OMB	Office of Management and Budget
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
PCI	Payment Card Industry
PDI	DISA Potential Discrepancy Item
RFC	Request for Comments
SCAP	Security Content Automation Protocol
SP	Service Pack
SP	Special Publication
STIG	Security Technical Implementation Guide
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VMS	DISA Vulnerability Management System
XCCDF	eXtensible Configuration Checklist Description Format
XML	eXtensible Markup Language

Appendix B—References and other Resources

Appendix B lists references and other resources related to SCAP 1.0 and its component specifications.

[BAR09] Barrett, M., Johnson, C., Mell, P., Quinn, S., and Scarfone, K., NIST Special Publication 800-117 (Draft), "Guide to Adopting and Using the Security Content Automation Protocol (SCAP)", May 2009, http://csrc.nist.gov/publications/drafts/800-117/draft-sp800-117.pdf

[BUT09] Buttner, A. and Ziring, N., "Common Platform Enumeration (CPE)—Specification, Version 2.2", MITRE Corporation, March 11, 2009. http://cpe.mitre.org/files/cpe-specification_2.2.pdf

[QUI08] Quinn, S. and Ziring, N., NIST Interagency Report 7275 Revision 3, "Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4", January 2008, http://csrc.nist.gov/publications/nistir/ir7275r3/NISTIR-7275r3.pdf

The resources below may be retrieved from the NIST SCAP web site:

[1] CVE specification and description (http://scap.nist.gov/revision/1.0/index.html#cve)

[2] CCE specification and description (http://scap.nist.gov/revision/1.0/index.html#cce)

[3] CPE specification and description (http://scap.nist.gov/revision/1.0/index.html#cpe)

[4] CVSS specification and description (http://scap.nist.gov/revision/1.0/index.html#cvss)

[5] XCCDF specification and description (http://scap.nist.gov/revision/1.0/index.html#xccdf)

[6] OVAL specification and description (http://scap.nist.gov/revision/1.0/index.html#oval)

Appendix C—SCAP Extensions to the XCCDF Specification

C.1 Rule and Group Selection

Rules and Groups may be selected for application in the context of either a Benchmark or a Profile contained by a Benchmark. This extension expands on the semantics of rule and group Selection.

C.1.1. A group or rule is selected in a Benchmark if and only if at least one of the following is true:

a. The group or rule is immediately contained by the Benchmark and the 'selected' attribute of the group or rule is bound to true.

b. The group or rule is immediately contained by a group that is selected in the Benchmark and the 'selected' attribute of the subject group or rule is bound to true.

c. The group or rule is selected by association relative[39] to the Benchmark.

C.1.2. A group or rule will be selected in a Profile only if it is either explicitly or implicitly selected in the Profile.

C.1.3. A group or rule is explicitly selected in a Profile only if there exists a `<select>` contained by the Profile whose 'idref' attribute is bound to the id of the group or rule and whose 'selected' attribute is set to true. A group or rule is explicitly deselected in a Profile only if there exists a `<select>` contained by the Profile whose 'idref' attribute is bound to the id of the group or rule and whose 'selected' attribute is set to false.

C.1.4. A group or rule is implicitly selected in a Profile if and only if it is not explicitly selected or deselected in the Profile and at least one of the following is true:

a. The group or rule is selected in the Benchmark.

b. The group or rule is selected in the Profile extended by the subject Profile.

c. The group or rule is selected by association relative to the Profile.

C.2 Selection by Association

The sequence of `<requires>` and `<conflicts>` optionally bound to a group or rule creates a set of directed associations rooted on the subject group or rule and terminating on other Groups or Rules. The resulting directed graphs are valid only if they are acyclic. The associations rooted on a group or rule may be used to determine an associative selection predicate on the subject group or rule. The selection predicate is evaluated as follows

C.2.1. The selection value of a `<requires>` relative to the Benchmark is true only if all of the Groups or Rules referenced by the element are selected by the Benchmark, likewise the selection value relative to a Profile is true only if all of the Groups or Rules referenced by the element are selected in the Profile.

C.2.2. The selection value of a `<conflicts>` relative to the Benchmark is true only if at least one of the Groups or Rules referenced by the element are deselected by the Benchmark, likewise the

[39] Selection by association is discussed in C.2.

selection value relative to a Profile is true only if at least one of the Groups or Rules referenced by the element are deselected in the Profile.

C.2.3. The selection value of a sequence of <requires> and <conflicts> is true relative to the Benchmark only if at least one of the elements in the sequence evaluates to true relative to the Benchmark, likewise the value of the sequence relative to a Profile is true only if at least one of the elements in the sequence evaluates to true relative to the Profile.

Appendix D—SCAP Compliance Verification Data Stream Example

The content in this XML example section has been derived from the NIST SP 800-68 configuration guidance for Windows XP operating systems. This example content is referenced throughout this document as an illustration of how a potential SCAP data stream may be represented. Please note that much of the content from the original source has been removed or changed. The complete, original data stream can be downloaded at http://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=76.

D.1 XCCDF Benchmark

The following example XCCDF XML instance represents a configuration checklist.

Figure D-1. example-winxp-xccdf.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Benchmark id="Windows-XP-sample" resolved="0" xml:lang="en"
  xmlns="http://checklists.nist.gov/xccdf/1.1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:cdf="http://checklists.nist.gov/xccdf/1.1" xmlns:cpe="http://cpe.mitre.org/dictionary/2.0"
  xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xhtml="http://www.w3.org/1999/xhtml"
  xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
  xsi:schemaLocation="http://checklists.nist.gov/xccdf/1.1 http://nvd.nist.gov/schema/xccdf-
1.1.4.xsd
      http://cpe.mitre.org/dictionary/2.0 http://cpe.mitre.org/files/cpe-dictionary 2.1.xsd">
  <status date="2009-09-18">draft</status>
  <title>Windows XP Configuration Verification Example</title>
  <description>This checklist has been created to assist IT professionals with understanding the
    requirements and conventions defined in the NIST SP 800-126.</description>
  <notice id="terms-of-use" xml:lang="en">Do not attempt to implement any of the settings in this
    guide without first testing them in a non-operational environment. NIST assumes no
    responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or
    implied, about its quality, reliability, or any other characteristic. NIST would appreciate
    acknowledgement if the document and template are used.</notice>
  <front-matter xml:lang="en">Example front matter</front-matter>
  <rear-matter xml:lang="en"><xhtml:strong>Trademark
    Information</xhtml:strong><xhtml:br/><xhtml:br/>Microsoft, Windows, Windows XP, Windows Vista,
    Internet Explorer, and Windows Firewall are either registered trademarks or trademarks of
    Microsoft Corporation in the United States and other countries.<xhtml:br/><xhtml:br/>All other
    names are registered trademarks or trademarks of their respective companies.</rear-matter>
  <reference href="http://nvd.nist.gov/chklst_detail.cfm?config_id=76">
    <dc:publisher>National Institute of Standards and Technology</dc:publisher>
    <dc:identifier>SP 800-68</dc:identifier>
  </reference>
  <platform idref="cpe:/o:microsoft:windows_xp"/>
  <version>v0.1</version>
  <metadata>
    <dc:creator>National Institute of Standards and Technology</dc:creator>
    <dc:publisher>National Institute of Standards and Technology</dc:publisher>
    <dc:contributor>John Doe</dc:contributor>
  </metadata>
  <!-- Scoring models supported by this checklist -->
  <model system="urn:xccdf:scoring:default"/>
  <model system="urn:xccdf:scoring:flat"/>
  <Profile id="example-profile-1">
    <title>Federal Desktop Core Configuration version 1.2.1.0</title>
    <description>This profile represents guidance outlined in Federal Desktop Core Configuration
      settings for desktop systems with Windows XP installed.</description>
    <!-- ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''' -->
    <!-- '''  2 - FDCC Security Settings                                                        ''' -->
    <!-- ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''' -->
    <!-- Account Lockout Policy Settings -->
    <select idref="account_lockout_duration" selected="true"/>
    <!--  Password Policy Settings  -->
    <select idref="minimum password length" selected="true"/>
    <!--  File System Policy  -->
    <select idref="regedit.exePermissions" selected="true"/>
```

```
    <!-- ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''' -->
    <!-- '''  4 - Fully Patched System                                                  ''' -->
    <!-- ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''' -->
    <select idref="security_patches_up_to_date" selected="true"/>
    <!-- ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''' -->
    <!-- ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''' -->
    <!-- ''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''' -->

    <refine-value idref="account_lockout_duration_var" selector="900_seconds"/>
    <refine-value idref="minimum_password_length_var" selector="12_characters"/>
  </Profile>
  <!-- This is an example of an XCCDF Group that contains only text. It can be used to represent
prose sections of the checklist document to support document generation. -->
  <Group id="introduction">
    <title xml:lang="en-US">Introduction</title>
    <description xml:lang="en-US">This is an example SCAP data stream for the Configuration
      Verfication use case. This data stream is based on the NIST SP 800-68. Please note that much
      of the content has been removed or changed. The complete, original data stream can be
      downloaded at:
      http://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=76.</description>
  </Group>
  <!-- ************************************************************************************* -->
  <!-- ***  5 - FDCC Security Settings                                                   *** -->
  <!-- ************************************************************************************* -->
  <Group id="security_settings">
    <title>Security Settings</title>
    <description>The following controls must be checked in order to verify compliance.</description>
    <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
    <!-- ~~~  Account Policies Group                                                        -->
    <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
    <Group id="account_policies_group">
      <title>Account Policies Group</title>
      <description>todo - description needed</description>
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!--           Account Lockout Policy Settings           -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <Group id="account_lockout_policy_settings">
        <title>Account Lockout Policy Settings</title>
        <description>Attackers often attempt to gain access to user accounts by guessing passwords.
          Windows XP can be configured to lock out (disable) an account when too many failed login
          attempts occur for a single user account in a certain time period. The following account
          lockout parameters are set in the NIST templates:<xhtml:p/>One of the main challenges in
          setting account policies is balancing security, functionality, and usability. For example,
          locking out user accounts after only a few failed logon attempts in a long time period may
          make it more difficult to gain unauthorized access to accounts by guessing passwords, but
          may also sharply increase the number of calls to the help desk to unlock accounts
          accidentally locked by failed attempts from legitimate users. This could also cause more
          users to write down their passwords or choose easier-to-remember passwords. Organizations
          should carefully think out such issues before setting Windows XP account
          policies.</description>
        <Value id="account_lockout_duration_var" type="number" operator="greater than or equal">
          <title>Account Lockout Duration</title>
          <description>The amount of time in seconds that an account is locked before it is
            automatically unlocked by the system. 15 minutes = 900 seconds A value of 0 means that
            an administrator must unlock the account.</description>
          <value>900</value>
          <value selector="admin_unlock">0</value>
          <value selector="900_seconds">900</value>
          <value selector="86400_seconds">86400</value>
        </Value>
        <Rule id="account_lockout_duration" selected="false" weight="10.0">
          <title>Account Lockout Duration</title>
          <description>The lockout duration specifies how long the user account should be locked out
            after too many bad logon attempts. This is often set to a low but substantial value
            (e.g., 15 minutes), for two reasons. First, a legitimate user that is accidentally
            locked out only has to wait 15 minutes to regain access, instead of asking an
            administrator to unlock the account. Second, an attacker who is guessing passwords using
            brute force methods will only be able to try a small number of passwords at a time, then
            wait 15 minutes before trying any more. This greatly reduces the chances that the brute
            force attack will be successful.</description>
          <reference>
```

```
            <dc:type>GPO</dc:type>
            <dc:source>Computer Configuration\Windows Settings\Security Settings\Account
              Policies\Account Lockout Policy</dc:source>
          </reference>
          <ident system="http://cce.mitre.org">CCE-2928-0</ident>
          <ident system="cce.mitre.org/version/4">CCE-980</ident>
          <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
            <check-export value-id="account lockout duration var"
              export-name="oval:gov.nist.fdcc.xp:var:15"/>
            <check-content-ref href="example-winxp-oval.xml" name="oval:gov.nist.fdcc.xp:def:23"/>
          </check>
        </Rule>
      </Group>
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!--              Password Policy Settings                    -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <Group id="password_policy_settings">
        <title>Password Policies</title>
        <description>In addition to educating users regarding the selection and use of good
          passwords, it is also important to set password parameters so that passwords are
          sufficiently strong. This reduces the likelihood of an attacker guessing or cracking
          passwords to gain unauthorized access to the system. As described in Section 3.2.1, NIST
          recommends the use of NTLM v2 or Kerberos instead of LM or NTLM v1 for authentication.
          Windows XP offers the same password parameters as Windows 2000. The following parameters
          are specified in the NIST templates:</description>
        <Value id="minimum_password_length_var" type="number" operator="greater than or equal">
          <title>Minimum Password Length</title>
          <description>The minimum number of characters required for a password</description>
          <value>8</value>
          <value selector="8_characters">8</value>
          <value selector="9_characters">9</value>
          <value selector="12_characters">12</value>
        </Value>
        <Rule id="minimum_password_length" selected="false" weight="10.0">
          <title>Minimum Password Length</title>
          <description>This setting specifies the minimum length of a password in characters. The
            rationale behind this setting is that longer passwords are more difficult to guess and
            crack than shorter passwords. The downside is that longer passwords are often more
            difficult for users to remember. Organizations that want to set a relatively large
            minimum password length should encourage their users to use passphrases, which may be
            easier to remember than conventional passwords.</description>
          <reference>
            <dc:type>GPO</dc:type>
            <dc:source>Computer Configuration\Windows Settings\Security Settings\Account
              Policies\Password Policy</dc:source>
          </reference>
          <ident system="http://cce.mitre.org">CCE-2981-9</ident>
          <ident system="cce.mitre.org/version/4">CCE-100</ident>
          <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
            <check-export value-id="minimum password length var"
              export-name="oval:gov.nist.fdcc.xp:var:12"/>
            <check-content-ref href="example-winxp-oval.xml" name="oval:gov.nist.fdcc.xp:def:19"/>
          </check>
        </Rule>
      </Group>
    </Group>
    <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
    <!-- ~~~  File Permissions Group ~~~ -->
    <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
    <Group id="file_permissions_group">
      <title>File Permission Settings</title>
      <description>This group checks the permissions of specified files.</description>
      <Rule id="regedit.exePermissions" selected="false" weight="10.0">
        <title>regedit.exe Permissions</title>
        <description>Failure to properly configure ACL file and directory permissions, allows the
          possibility of unauthorized and anonymous modification to the operating system and
          installed applications.</description>
        <reference>
          <dc:type>GPO</dc:type>
          <dc:source>Computer Configuration\Windows Settings\Security Settings\File
            System</dc:source>
```

```
        </reference>
        <ident system="http://cce.mitre.org">CCE-2175-8</ident>
        <ident system="cce.mitre.org/version/4">CCE-795</ident>
        <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
          <check-content-ref href="example-winxp-oval.xml" name="oval:gov.nist.fdcc.xp:def:146"/>
        </check>
      </Rule>
    </Group>
  </Group>
  <!-- **************************** -->
  <!-- ***  7 - Security Patches *** -->
  <!-- **************************** -->
  <Group id="security_patches">
    <title>Security Patches</title>
    <description>Securing a given computer has become increasingly important. As such, it is
      essential to keep a host up to current patch levels to eliminate known vulnerabilities and
      weaknesses. In conjunction with antivirus software and a personal firewall, patching goes a
      long way to securing a host against outside attacks and exploitation. Microsoft provides two
      mechanisms for distributing security updates: Automatic Updates and Microsoft Update. In
      smaller environments, either method may be sufficient for keeping systems current with
      patches. Other environments typically have a software change management control process or a
      patch management program that tests patches before deploying them; distribution may then occur
      through local Windows Update Services (WUS) or Windows Server Update Services (WSUS) servers,
      which provide approved security patches for use by the Automatic Updates
      feature.</description>
    <Rule id="security_patches_up_to_date" selected="false" weight="10.0">
      <title>Security Patches Up-To-Date</title>
      <description>Keep systems up to current patch levels to eliminate known vulnerabilities and
        weaknesses.</description>
      <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
        <check-content-ref href="http://nvd.nist.gov/scap/content/fdcc-winxp-patches.xml"/>
        <check-content-ref href="example-winxp-patches.xml"/>
      </check>
    </Rule>
  </Group>
  <!-- ================================================================================== -->
  <!-- ================================================================================== -->
  <!-- ================================================================================== -->
</Benchmark>
```

D.2 OVAL Compliance

The following OVAL XML instance represents compliance definitions used to evaluate the XCCDF checklist from the previous section.

Figure D-2. example-winxp-oval.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
  xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
  xmlns:ind-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/windows-
definitions-schema.xsd
      http://oval.mitre.org/XMLSchema/oval-definitions-5#independent
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/independent-
definitions-schema.xsd
      http://oval.mitre.org/XMLSchema/oval-definitions-5
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/oval-
definitions-schema.xsd
      http://oval.mitre.org/XMLSchema/oval-common-5
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/oval-common-
schema.xsd">
  <generator>
    <oval:product name>National Institute of Standards and Technology</oval:product name>
    <oval:schema_version>5.3</oval:schema_version>
    <oval:timestamp>2009-04-08T15:04:22.000-05:00</oval:timestamp>
  </generator>
  <!-- ================================================================================ -->
  <!-- ================================  DEFINITIONS  ================================= -->
  <!-- ================================================================================ -->
  <definitions>
    <definition id="oval:gov.nist.fdcc.xp:def:23" version="1" class="compliance">
      <metadata>
        <title>Account Lockout Duration</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
        </affected>
        <reference source="http://cce.mitre.org" ref_id="CCE-2928-0"/>
        <reference source="cce.mitre.org/version/4" ref_id="CCE-980"/>
        <description>This definition verifies that locked accounts remains locked for the defined
          number of minutes before they are automatically unlocked.</description>
      </metadata>
      <criteria>
        <extend_definition comment="Microsoft Windows XP is installed"
          definition_ref="oval:gov.nist.fdcc.xp:def:2"/>
        <criteria operator="OR">
          <criterion
            comment="Account Lockout Duration is set to keep accounts locked for at least the
defined number of minutes"
            test_ref="oval:gov.nist.fdcc.xp:tst:19"/>
          <criterion
            comment="Account Lockout Duration is set to keep accounts locked until an
administrator unlocks them"
            test_ref="oval:gov.nist.fdcc.xp:tst:1911"/>
        </criteria>
      </criteria>
    </definition>
    <definition id="oval:gov.nist.fdcc.xp:def:19" version="1" class="compliance">
      <metadata>
        <title>Minimum Password Length</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
        </affected>
        <reference source="http://cce.mitre.org" ref_id="CCE-2981-9"/>
```

```
        <reference source="cce.mitre.org/version/4" ref_id="CCE-100"/>
        <description>Minimum password length is the profile defined number of
          characters</description>
      </metadata>
      <criteria>
        <extend_definition comment="Microsoft Windows XP is installed"
          definition_ref="oval:gov.nist.fdcc.xp:def:2"/>
        <criterion comment="Minimum password length is profile defined"
          test_ref="oval:gov.nist.fdcc.xp:tst:15"/>
      </criteria>
    </definition>
    <definition id="oval:gov.nist.fdcc.xp:def:146" version="1" class="compliance">
      <metadata>
        <title>Administrators and System User Have Full Access to the SYSTEMROOT/regedit.exe
          File</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
        </affected>
        <reference source="http://cce.mitre.org" ref_id="CCE-2175-8"/>
        <reference source="cce.mitre.org/version/4" ref_id="CCE-795"/>
        <description>The Administrators group and the System user should have full access to the
          SYSTEMROOT/regedit.exe file and all other users should have no file access
          privileges</description>
      </metadata>
      <criteria>
        <extend_definition comment="Microsoft Windows XP is installed"
          definition_ref="oval:gov.nist.fdcc.xp:def:2"/>
        <criteria operator="AND">
          <criterion
            comment="The Administrators group is granted full access to the file regedit.exe"
            test_ref="oval:gov.nist.fdcc.xp:tst:248"/>
          <criterion comment="The System user is granted full access to the file regedit.exe"
            test_ref="oval:gov.nist.fdcc.xp:tst:249"/>
          <criterion
            comment="There are no access privileges to file regedit.exe by users not part of the
Administrators group or the System user"
            test_ref="oval:gov.nist.fdcc.xp:tst:250"/>
        </criteria>
      </criteria>
    </definition>

    <!--------------------------------------------------------------------------------->
    <!--------------------------  EXTENDED DEFINITIONS  ------------------------------->
    <!--------------------------------------------------------------------------------->
    <definition id="oval:gov.nist.fdcc.xp:def:2" version="1" class="inventory">
      <metadata>
        <title>Microsoft Windows XP is installed</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
        </affected>
        <description>Microsoft Windows XP is installed</description>
      </metadata>
      <criteria>
        <criterion comment="the installed operating system is part of the Microsoft Windows
family"
          test_ref="oval:gov.nist.fdcc.xp:tst:6"/>
        <criterion comment="Microsoft Windows XP is installed"
          test_ref="oval:gov.nist.fdcc.xp:tst:7"/>
      </criteria>
    </definition>
  </definitions>
  <!-- ================================================================================= -->
  <!-- ================================  TESTS  ======================================== -->
  <!-- ================================================================================= -->
  <tests>
    <family_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
      id="oval:gov.nist.fdcc.xp:tst:6" version="1"
      comment="the installed operating system is part of the Microsoft Windows family"
      check_existence="at_least_one_exists" check="only one">
      <object object_ref="oval:gov.nist.fdcc.xp:obj:3"/>
      <state state_ref="oval:gov.nist.fdcc.xp:ste:14"/>
```

```
    </family_test>
    <registry test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:tst:7" version="1" comment="Microsoft Windows XP is installed"
      check existence="at least one exists" check="at least one">
      <object object_ref="oval:gov.nist.fdcc.xp:obj:4"/>
      <state state_ref="oval:gov.nist.fdcc.xp:ste:15"/>
    </registry_test>
    <passwordpolicy test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:tst:15" version="1"
      comment="Minimum password length is profile defined" check existence="at least one exists"
      check="all">
      <object object_ref="oval:gov.nist.fdcc.xp:obj:8"/>
      <state state_ref="oval:gov.nist.fdcc.xp:ste:20"/>
    </passwordpolicy test>
    <lockoutpolicy_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:tst:19" version="1"
      comment="Account Lockout Duration is set to keep accounts locked for at least the defined
number of minutes"
      check_existence="at_least_one_exists" check="all">
      <object object_ref="oval:gov.nist.fdcc.xp:obj:9"/>
      <state state_ref="oval:gov.nist.fdcc.xp:ste:25"/>
    </lockoutpolicy test>
    <lockoutpolicy_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:tst:1911" version="1"
      comment="Account Lockout Duration is set to keep accounts locked until an administrator
unlocks them"
      check existence="at least one exists" check="all">
      <object object_ref="oval:gov.nist.fdcc.xp:obj:9"/>
      <state state_ref="oval:gov.nist.fdcc.xp:ste:2511"/>
    </lockoutpolicy_test>
    <fileeffectiverights53_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:tst:248" version="1"
      comment="The Administrators group is granted full access to the file regedit.exe"
      check_existence="any_exist" check="all">
      <object object_ref="oval:gov.nist.fdcc.xp:obj:155"/>
      <state state_ref="oval:gov.nist.fdcc.xp:ste:51"/>
    </fileeffectiverights53_test>
    <fileeffectiverights53 test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:tst:249" version="1"
      comment="The System user is granted full access to the file regedit.exe"
      check_existence="any_exist" check="all">
      <object object_ref="oval:gov.nist.fdcc.xp:obj:156"/>
      <state state ref="oval:gov.nist.fdcc.xp:ste:51"/>
    </fileeffectiverights53_test>
    <fileeffectiverights53_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:tst:250" version="1"
      comment="There are no access privileges to file regedit.exe by users not part of the
Administrators group or the System user"
      check existence="any exist" check="all">
      <object object_ref="oval:gov.nist.fdcc.xp:obj:157"/>
      <state state_ref="oval:gov.nist.fdcc.xp:ste:52"/>
    </fileeffectiverights53_test>
  </tests>
  <!-- ================================================================================ -->
  <!-- ================================  OBJECTS  ================================== -->
  <!-- ================================================================================ -->
  <objects>
    <family_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
      id="oval:gov.nist.fdcc.xp:obj:3" version="1"/>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:obj:4" version="1">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SOFTWARE\Microsoft\Windows NT\CurrentVersion</key>
      <name>CurrentVersion</name>
    </registry object>
    <passwordpolicy_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:obj:8" version="1"/>
    <lockoutpolicy_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
```

```
      id="oval:gov.nist.fdcc.xp:obj:9" version="1"/>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:obj:79" version="1">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SOFTWARE\Microsoft\Windows NT\CurrentVersion</key>
      <name>SystemRoot</name>
    </registry_object>
    <fileeffectiverights53_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:obj:155" version="1">
      <path datatype="string" var_ref="oval:gov.nist.fdcc.xp:var:4"/>
      <filename>regedit.exe</filename>
      <trustee_sid>S-1-5-32-544</trustee_sid>
    </fileeffectiverights53_object>
    <fileeffectiverights53_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:obj:156" version="1">
      <path datatype="string" var_ref="oval:gov.nist.fdcc.xp:var:4"/>
      <filename>regedit.exe</filename>
      <trustee_sid>S-1-5-18</trustee_sid>
    </fileeffectiverights53_object>
    <fileeffectiverights53_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:obj:157" version="1">
      <set xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
set_operator="INTERSECTION">
        <set set_operator="COMPLEMENT">
          <object_reference>oval:gov.nist.fdcc.xp:obj:318</object_reference>
          <object_reference>oval:gov.nist.fdcc.xp:obj:156</object_reference>
        </set>
        <set set_operator="COMPLEMENT">
          <object_reference>oval:gov.nist.fdcc.xp:obj:318</object_reference>
          <object_reference>oval:gov.nist.fdcc.xp:obj:158</object_reference>
        </set>
      </set>
    </fileeffectiverights53_object>
    <fileeffectiverights53_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:obj:318" version="1">
      <behaviors resolve_group="true"/>
      <path datatype="string" var_ref="oval:gov.nist.fdcc.xp:var:4"/>
      <filename>regedit.exe</filename>
      <trustee_sid operation="pattern match">.*</trustee_sid>
    </fileeffectiverights53_object>
    <fileeffectiverights53_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:obj:158" version="1">
      <behaviors resolve_group="true"/>
      <path datatype="string" var_ref="oval:gov.nist.fdcc.xp:var:4"/>
      <filename>regedit.exe</filename>
      <trustee_sid>S-1-5-32-544</trustee_sid>
    </fileeffectiverights53_object>
  </objects>
  <!-- ================================================================================ -->
  <!-- ================================  STATES  ================================== -->
  <!-- ================================================================================ -->
  <states>
    <family_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
      id="oval:gov.nist.fdcc.xp:ste:14" version="1">
      <family>windows</family>
    </family_state>
    <passwordpolicy_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:ste:20" version="1">
      <min_passwd_len datatype="int" operation="greater_than_or_equal"
        var_ref="oval:gov.nist.fdcc.xp:var:12"/>
    </passwordpolicy_state>
    <lockoutpolicy_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:ste:25" version="1">
      <lockout_duration datatype="int" operation="greater_than_or_equal"
        var_ref="oval:gov.nist.fdcc.xp:var:15"/>
    </lockoutpolicy_state>
```

```
    <lockoutpolicy_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:ste:2511" version="1">
      <lockout_duration datatype="int">-1</lockout_duration>
    </lockoutpolicy state>
    <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.xp:ste:15" version="1">
      <value datatype="string">5.1</value>
    </registry state>
    <fileeffectiverights53_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:ste:51" version="1"
      comment="specified account is granted full control">
      <standard_delete datatype="boolean">1</standard_delete>
      <standard read control datatype="boolean">1</standard read control>
      <standard_write_dac datatype="boolean">1</standard_write_dac>
      <standard write owner datatype="boolean">1</standard write owner>
      <standard_synchronize datatype="boolean">1</standard_synchronize>
      <file_read_data datatype="boolean">1</file_read_data>
      <file_write_data datatype="boolean">1</file_write_data>
      <file_append_data datatype="boolean">1</file_append_data>
      <file_read_ea datatype="boolean">1</file_read_ea>
      <file write ea datatype="boolean">1</file write ea>
      <file_execute datatype="boolean">1</file_execute>
      <file_delete_child datatype="boolean">1</file_delete_child>
      <file read attributes datatype="boolean">1</file read attributes>
      <file_write_attributes datatype="boolean">1</file_write_attributes>
    </fileeffectiverights53 state>
    <fileeffectiverights53_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-
5#windows"
      id="oval:gov.nist.fdcc.xp:ste:52" version="1"
      comment="specified account has no access privileges">
      <standard_delete datatype="boolean">0</standard_delete>
      <standard read control datatype="boolean">0</standard read control>
      <standard_write_dac datatype="boolean">0</standard_write_dac>
      <standard_write_owner datatype="boolean">0</standard_write_owner>
      <standard_synchronize datatype="boolean">0</standard_synchronize>
      <access_system_security datatype="boolean">0</access_system_security>
      <generic_read datatype="boolean">0</generic_read>
      <generic write datatype="boolean">0</generic write>
      <generic_execute datatype="boolean">0</generic_execute>
      <generic_all datatype="boolean">0</generic_all>
      <file_read_data datatype="boolean">0</file_read_data>
      <file_write_data datatype="boolean">0</file_write_data>
      <file_append_data datatype="boolean">0</file_append_data>
      <file read ea datatype="boolean">0</file read ea>
      <file_write_ea datatype="boolean">0</file_write_ea>
      <file_execute datatype="boolean">0</file_execute>
      <file_delete_child datatype="boolean">0</file_delete_child>
      <file_read_attributes datatype="boolean">0</file_read_attributes>
      <file write attributes datatype="boolean">0</file write attributes>
    </fileeffectiverights53_state>
  </states>
  <!-- ================================================================================ -->
  <!-- ================================  VARIABLES  ================================== -->
  <!-- ================================================================================ -->
  <variables>
    <local_variable id="oval:gov.nist.fdcc.xp:var:1" version="1"
      comment="Windows system32 directory" datatype="string">
      <concat>
        <object_component object_ref="oval:gov.nist.fdcc.xp:obj:79" item_field="value"/>
        <literal_component>\system32</literal_component>
      </concat>
    </local_variable>
    <local variable id="oval:gov.nist.fdcc.xp:var:4" version="1" comment="Windows directory"
      datatype="string">
      <object_component object_ref="oval:gov.nist.fdcc.xp:obj:79" item_field="value"/>
    </local_variable>
    <external variable id="oval:gov.nist.fdcc.xp:var:12" version="1"
      comment="minimum password length" datatype="int"/>
    <external variable id="oval:gov.nist.fdcc.xp:var:15" version="1"
      comment="Account lockout duration" datatype="int"/>
```

```
  </variables>
  <!-- ================================================================================ -->
  <!-- ================================================================================ -->
  <!-- ================================================================================ -->
</oval_definitions>
```

D.3 OVAL Patch

The following OVAL XML instance represents patch definitions used to assess the *<xccdf:Rule>* element from section D.1 lines 223-226.

Figure D-3. example-winxp-patches.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
  xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:ind-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
  xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-common-5
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/oval-common-
schema.xsd
  http://oval.mitre.org/XMLSchema/oval-definitions-5
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/oval-
definitions-schema.xsd
  http://oval.mitre.org/XMLSchema/oval-definitions-5#windows
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/windows-
definitions-schema.xsd
  http://oval.mitre.org/XMLSchema/oval-definitions-5#independent
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/independent-
definitions-schema.xsd">
  <generator>
    <oval:product_name>National Institute of Standards and Technology</oval:product_name>
    <oval:schema_version>5.3</oval:schema_version>
    <oval:timestamp>2009-08-21T08:34:35.000-05:00</oval:timestamp>
  </generator>
  <!-- ================================================================================ -->
  <!-- ================================  DEFINITIONS  ================================= -->
  <!-- ================================================================================ -->
  <definitions>
    <definition id="oval:gov.nist.fdcc.patch:def:5" version="0" class="patch">
      <metadata>
        <title>MS05-013: Vulnerability in the DHTML Editing Component ActiveX Control Could Allow
          Remote Code Execution (891781)</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
          <product>Microsoft Internet Explorer</product>
        </affected>
        <reference source="Microsoft" ref_id="MS05-013"
          ref_url="http://www.microsoft.com/technet/security/bulletin/ms05-013.mspx"/>
        <reference source="Microsoft" ref_id="KB891781"
          ref_url="http://support.microsoft.com/kb/891781"/>
        <reference source="Bugtraq ID" ref_id="11950"
          ref_url="http://www.securityfocus.com/bid/11950"/>
        <reference source="CERT-VN" ref_id="VU#356600"
          ref_url="http://www.kb.cert.org/vuls/id/356600"/>
        <reference source="CIAC" ref_id="p-126"
          ref_url="http://www.ciac.org/ciac/bulletins/p-126.shtml"/>
        <reference source="CVE" ref_id="CVE-2004-1319"
          ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1319"/>
        <reference source="OVAL" ref_id="oval:org.mitre.oval:def:3851"

ref_url="http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3851"/>
        <reference source="OVAL" ref_id="oval:org.mitre.oval:def:1701"

ref_url="http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1701"/>
        <reference source="OVAL" ref_id="oval:org.mitre.oval:def:4758"

ref_url="http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4758"/>
        <reference source="OVAL" ref_id="oval:org.mitre.oval:def:1114"

ref_url="http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1114"/>
        <reference source="OVAL" ref_id="oval:org.mitre.oval:def:3464"
```

```
ref url="http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3464"/>
        <description>Microsoft has released MS05-013 to address security issues in Microsoft
          Internet Explorer as documented by CVE-2004-1319.</description>
      </metadata>
      <criteria comment="Software section" operator="AND">
        <extend_definition comment="Microsoft Windows XP (32-bit) SP2 is installed"
          definition ref="oval:gov.nist.fdcc.patch:def:115276"/>
        <criterion comment="the version of dhtmled.ocx is less than 6.1.0.9232" negate="false"
          test ref="oval:org.mitre.oval:tst:427"/>
        <criterion comment="the patch kb891781 is installed (Hotfix key)" negate="true"
          test_ref="oval:org.mitre.oval:tst:1151"/>
      </criteria>
    </definition>
    <definition id="oval:gov.nist.fdcc.patch:def:1784" version="2" class="patch">
      <metadata>
        <title>MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code
Execution
          (938127)</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
          <platform>Microsoft Windows Vista</platform>
          <product>Microsoft Internet Explorer</product>
        </affected>
        <reference source="Microsoft" ref id="MS07-050"
          ref_url="http://www.microsoft.com/technet/security/bulletin/MS07-050.mspx"/>
        <reference source="Microsoft" ref id="938127"
          ref url="http://support.microsoft.com/kb/938127"/>
        <reference source="CVE" ref_id="CVE-2007-1749"
          ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1749"/>
        <reference source="OVAL" ref_id="oval:org.mitre.oval:def:1784"

ref url="http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1784"/>
        <description>Microsoft has released MS07-050 to address security issues in the Vector
Markup
          Language (VML) implementation in Windows as documented by CVE-2007-1749.</description>
      </metadata>
      <criteria operator="OR">
        <criteria comment="IE 6 on Win XP SP2" operator="AND">
          <extend_definition comment="Microsoft Windows XP (32-bit) SP2 is installed"
            definition_ref="oval:gov.nist.fdcc.patch:def:115276"/>
          <extend_definition definition_ref="oval:org.mitre.oval:def:563"
            comment="Internet Explorer 6 is installed"/>
          <criterion comment="the version of vgx.dll is less than 6.0.2900.3164"
            test ref="oval:org.mitre.oval:tst:3856"/>
        </criteria>
        <criteria comment="IE 7 on Win XP SP2" operator="AND">
          <extend_definition comment="Microsoft Windows XP (32-bit) SP2 is installed"
            definition_ref="oval:gov.nist.fdcc.patch:def:115276"/>
          <extend definition definition ref="oval:org.mitre.oval:def:627"
            comment="Internet Explorer 7 is installed"/>
          <criterion comment="the version of vgx.dll is less than 7.0.6000.20628"
            test_ref="oval:org.mitre.oval:tst:4182"/>
        </criteria>
        <criteria comment="IE 6 on Win XP SP2 (64-bit)" operator="AND">
          <extend definition comment="Microsoft Windows XP SP2 (64-bit) is installed"
            definition_ref="oval:gov.nist.fdcc.patch:def:115277"/>
          <extend definition comment="Internet Explorer 6 is installed"
            definition_ref="oval:org.mitre.oval:def:563"/>
          <criterion comment="the version of vgx.dll is less than 6.0.3790.4106"
            test_ref="oval:org.mitre.oval:tst:3422"/>
        </criteria>
        <criteria comment="IE 7 on Win XP SP2 (64-bit)" operator="AND">
          <extend definition comment="Microsoft Windows XP SP2 (64-bit) is installed"
            definition_ref="oval:gov.nist.fdcc.patch:def:115277"/>
          <extend_definition definition_ref="oval:org.mitre.oval:def:627"
            comment="Internet Explorer 7 is installed"/>
          <criterion comment="the version of vgx.dll is less than 7.0.6000.20628"
            test_ref="oval:org.mitre.oval:tst:4182"/>
        </criteria>
      </criteria>
```

```
    </definition>

    <!-- ================================================================================ -->
    <!-- ========================  EXTENDED DEFINITIONS  ============================== -->
    <!-- ================================================================================ -->
    <definition id="oval:gov.nist.fdcc.patch:def:115275" version="0" class="inventory">
      <metadata>
        <title>Microsoft Windows XP is installed</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
        </affected>
        <reference source="CPE" ref_id="cpe:/o:microsoft:windows_xp"/>
        <description>The operating system installed on the system is Microsoft Windows
          XP.</description>
      </metadata>
      <criteria operator="AND">
        <criterion comment="the installed operating system is part of the Microsoft Windows
family"
          test_ref="oval:org.mitre.oval:tst:99"/>
        <criterion comment="Windows XP is installed"
test_ref="oval:gov.nist.fccc.patch:tst:57914"/>
        <criterion comment="Currentversion = 5.1 or 5.2"
          test_ref="oval:gov.nist.fdcc.patch:tst:115300"/>
      </criteria>
    </definition>
    <definition id="oval:gov.nist.fdcc.patch:def:115276" version="0" class="inventory">
      <metadata>
        <title>Microsoft Windows XP (32-bit) SP2 is installed</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
        </affected>
        <reference source="CPE" ref_id="cpe:/o:microsoft:windows_xp::sp2:x86"/>
        <description>A version of Microsoft Windows XP (32-bit) SP2 is installed.</description>
      </metadata>
      <criteria operator="AND">
        <extend_definition comment="Microsoft Windows XP is installed"
          definition_ref="oval:gov.nist.fdcc.patch:def:115275"/>
        <criterion comment="a version of Windows for the x86 architecture is installed"
          test_ref="oval:org.mitre.oval:tst:3823"/>
        <criterion comment="Win2K/XP/2003 service pack 2 is installed"
          test_ref="oval:org.mitre.oval:tst:3019"/>
      </criteria>
    </definition>
    <definition id="oval:gov.nist.fdcc.patch:def:115277" version="0" class="inventory">
      <metadata>
        <title>Microsoft Windows XP (64-bit) SP2 is installed</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
        </affected>
        <reference source="CPE" ref_id="cpe:/o:microsoft:windows_xp::sp2:x64"/>
        <description>A version of Microsoft Windows XP (64-bit) SP2 is installed.</description>
      </metadata>
      <criteria operator="AND">
        <extend_definition comment="Microsoft Windows XP is installed"
          definition_ref="oval:gov.nist.fdcc.patch:def:115275"/>
        <criterion comment="a version of Windows for the x64 architecture is installed"
          test_ref="oval:org.mitre.oval:tst:3653"/>
        <criterion comment="Win2K/XP/2003 service pack 2 is installed"
          test_ref="oval:org.mitre.oval:tst:3019"/>
      </criteria>
    </definition>
    <definition id="oval:org.mitre.oval:def:563" version="3" class="inventory">
      <metadata>
        <title>Microsoft Internet Explorer 6 is installed</title>
        <affected family="windows">
          <platform>Microsoft Windows 2000</platform>
          <platform>Microsoft Windows XP</platform>
          <platform>Microsoft Windows Server 2003</platform>
        </affected>
        <reference source="CPE" ref_id="cpe:/a:microsoft:ie:6"/>
        <description>The application Microsoft Internet Explorer 6 is installed.</description>
```

```
        <oval_repository>
          <dates>
            <submitted date="2006-08-11T12:53:40">
              <contributor organization="ThreatGuard, Inc.">Robert L. Hollis</contributor>
            </submitted>
            <status_change date="2006-09-08T11:26:00.000-04:00">DRAFT</status_change>
            <status_change date="2006-09-27T12:29:31.086-04:00">INTERIM</status_change>
            <status change date="2006-10-16T15:58:44.500-04:00">ACCEPTED</status change>
            <modified comment="Added an anchor to the regex used to check for Internet Explorer
6."
              date="2007-01-11T20:38:00.950-05:00">
              <contributor organization="The MITRE Corporation">Matthew Wojcik</contributor>
            </modified>
            <status change date="2007-01-11T20:49:17.329-05:00">INTERIM</status change>
            <status_change date="2007-02-20T13:40:46.580-05:00">ACCEPTED</status_change>
            <modified comment="Added CPE reference." date="2007-04-30T07:48:00.756-04:00">
              <contributor organization="The MITRE Corporation">Jonathan Baker</contributor>
            </modified>
            <status_change date="2007-04-30T07:54:07.779-04:00">INTERIM</status_change>
            <status_change date="2007-05-23T15:05:48.577-04:00">ACCEPTED</status_change>
          </dates>
          <status>ACCEPTED</status>
        </oval_repository>
      </metadata>
      <criteria>
        <criterion comment="Internet Explorer 6 (any patch level) is installed"
          test ref="oval:org.mitre.oval:tst:2333"/>
      </criteria>
    </definition>
    <definition id="oval:org.mitre.oval:def:627" version="1" class="inventory">
      <metadata>
        <title>Microsoft Internet Explorer 7 is installed</title>
        <affected family="windows">
          <platform>Microsoft Windows XP</platform>
          <platform>Microsoft Windows Server 2003</platform>
          <platform>Microsoft Windows Vista</platform>
        </affected>
        <reference source="CPE" ref_id="cpe:/a:microsoft:ie:7"/>
        <description>A version of Microsoft Internet Explorer 7 is installed.</description>
        <oval_repository>
          <dates>
            <submitted date="2007-01-09T06:00:00">
              <contributor organization="Secure Elements, Inc.">Sudhir Gandhe</contributor>
            </submitted>
            <status change date="2007-01-11T15:30:00-04:00">DRAFT</status change>
            <status_change date="2007-02-20T13:40:49.320-05:00">INTERIM</status_change>
            <modified comment="Added Microsoft Windows Vista to the list of affected platforms."
              date="2007-03-05T09:10:00.104-05:00">
              <contributor organization="The MITRE Corporation">Andrew Buttner</contributor>
            </modified>
            <status_change date="2007-03-21T16:17:23.092-04:00">ACCEPTED</status_change>
          </dates>
          <status>ACCEPTED</status>
        </oval_repository>
      </metadata>
      <criteria>
        <criterion comment="Internet Explorer 7 is installed"
test ref="oval:org.mitre.oval:tst:178"
        />
      </criteria>
    </definition>
  </definitions>
  <!-- ================================================================================ -->
  <!-- ================================  TESTS  ======================================= -->
  <!-- ================================================================================ -->
  <tests>
    <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fccc.patch:tst:57914" version="0" comment="Windows XP is installed"
      check_existence="at_least_one_exists" check="at least one">
      <object object ref="oval:org.mitre.oval:obj:5590"/>
      <state state_ref="oval:gov.nist.fccc.patch:ste:53828"/>
```

```
    </registry_test>
    <family test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
      id="oval:org.mitre.oval:tst:99" version="1"
      comment="the installed operating system is part of the Microsoft Windows family"
      check_existence="at_least_one_exists" check="only one">
      <object object_ref="oval:org.mitre.oval:obj:99"/>
      <state state_ref="oval:org.mitre.oval:ste:99"/>
    </family test>
    <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:178" version="1" comment="Internet Explorer 7 is installed"
      check_existence="at_least_one_exists" check="at least one">
      <object object_ref="oval:org.mitre.oval:obj:247"/>
      <state state_ref="oval:org.mitre.oval:ste:115"/>
    </registry test>
    <file_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:427" version="1"
      comment="the version of dhtmled.ocx is less than 6.1.0.9232"
      check_existence="at_least_one_exists" check="all">
      <object object_ref="oval:org.mitre.oval:obj:377"/>
      <state state_ref="oval:org.mitre.oval:ste:394"/>
    </file_test>
    <registry test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:1151" version="2"
      comment="the patch kb891781 is installed (Hotfix key)"
check existence="at least one exists"
      check="at least one">
      <object object ref="oval:org.mitre.oval:obj:823"/>
      <state state_ref="oval:org.mitre.oval:ste:1031"/>
    </registry_test>
    <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:2333" version="2"
      comment="Internet Explorer 6 (any patch level) is installed"
      check existence="at least one exists" check="at least one">
      <object object_ref="oval:org.mitre.oval:obj:247"/>
      <state state_ref="oval:org.mitre.oval:ste:2185"/>
    </registry_test>
    <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:3019" version="1"
      comment="Win2K/XP/2003 service pack 2 is installed" check existence="at least one exists"
      check="at least one">
      <object object_ref="oval:org.mitre.oval:obj:717"/>
      <state state_ref="oval:org.mitre.oval:ste:2827"/>
    </registry_test>
    <file_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:3422" version="3"
      comment="the version of vgx.dll is less than 6.0.3790.4106"
      check_existence="at_least_one_exists" check="at least one">
      <object object_ref="oval:org.mitre.oval:obj:308"/>
      <state state_ref="oval:org.mitre.oval:ste:3490"/>
    </file test>
    <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:3653" version="2"
      comment="a version of Windows for the x64 architecture is installed"
      check_existence="at_least_one_exists" check="at least one">
      <object object_ref="oval:org.mitre.oval:obj:1576"/>
      <state state ref="oval:org.mitre.oval:ste:3180"/>
    </registry_test>
    <registry test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:3823" version="1"
      comment="a version of Windows for the x86 architecture is installed"
      check_existence="at_least_one_exists" check="at least one">
      <object object ref="oval:org.mitre.oval:obj:1576"/>
      <state state_ref="oval:org.mitre.oval:ste:3649"/>
    </registry test>
    <file_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:3856" version="3"
      comment="the version of vgx.dll is less than 6.0.2900.3164"
      check existence="at least one exists" check="at least one">
      <object object_ref="oval:org.mitre.oval:obj:308"/>
      <state state ref="oval:org.mitre.oval:ste:3185"/>
    </file_test>
```

```
    <file_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:tst:4182" version="3"
      comment="the version of vgx.dll is less than 7.0.6000.20628"
      check_existence="at_least_one_exists" check="at least one">
      <object object_ref="oval:org.mitre.oval:obj:308"/>
      <state state_ref="oval:org.mitre.oval:ste:3412"/>
    </file_test>
    <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.patch:tst:115300" version="0"
      comment="a version of Microsoft Windows XP is installed"
check_existence="at_least_one_exists"
      check="at least one">
      <object object_ref="oval:org.mitre.oval:obj:123"/>
      <state state_ref="oval:gov.nist.fdcc.patch:ste:115263"/>
    </registry_test>
  </tests>
  <!-- ================================================================================ -->
  <!-- ================================  OBJECTS  ================================== -->
  <!-- ================================================================================ -->
  <objects>
    <family_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
      id="oval:org.mitre.oval:obj:99" version="1"
      comment="This is the default family object. Only one family object should exist."/>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:123" version="1"
      comment="Registry key that hold the current windows os version">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SOFTWARE\Microsoft\Windows NT\CurrentVersion</key>
      <name>CurrentVersion</name>
    </registry_object>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:247" version="1"
      comment="This registry key identifies the version of internet Explorer">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SOFTWARE\Microsoft\Internet Explorer</key>
      <name>Version</name>
    </registry_object>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:281" version="1"
      comment="The registry key that identifies the location of the common files directory.">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SOFTWARE\Microsoft\Windows\CurrentVersion</key>
      <name>CommonFilesDir</name>
    </registry_object>
    <file object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:308" version="2">
      <path var_ref="oval:org.mitre.oval:var:209" var_check="all"/>
      <filename>vgx.dll</filename>
    </file_object>
    <file object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:377" version="1">
      <path var ref="oval:org.mitre.oval:var:206" var check="all"/>
      <filename>dhtmled.ocx</filename>
    </file_object>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:717" version="1"
      comment="This registry key holds the service pack installed on the host if one is
present.">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SOFTWARE\Microsoft\Windows NT\CurrentVersion</key>
      <name>CSDVersion</name>
    </registry object>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:823" version="2">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key operation="equals">SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\KB891781</key>
      <name operation="equals">IsInstalled</name>
    </registry object>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:1576" version="1"
      comment="This registry key identifies the architecture on the system">
```

```
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SYSTEM\CurrentControlSet\Control\Session Manager\Environment</key>
      <name>PROCESSOR_ARCHITECTURE</name>
    </registry object>
    <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:obj:5590" version="1" comment="This registry key  ProductName">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SOFTWARE\Microsoft\Windows NT\CurrentVersion</key>
      <name>ProductName</name>
    </registry object>
  </objects>
  <!-- ================================================================================ -->
  <!-- ================================  STATES  ================================== -->
  <!-- ================================================================================ -->
  <states>
    <registry state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fccc.patch:ste:53828" version="0" comment="The registry key matches with
XP">
      <value operation="pattern match">.*[XPxp].*</value>
    </registry_state>
    <family_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
      id="oval:org.mitre.oval:ste:99" version="1" comment="Microsoft Windows family">
      <family>windows</family>
    </family_state>
    <registry state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:115" version="1"
      comment="The registry key has a value that matches 7.*">
      <value operation="pattern match">^7\..*$</value>
    </registry_state>
    <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:1031" version="1">
      <value operation="equals" datatype="int">1</value>
    </registry state>
    <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:2185" version="2"
      comment="The registry key has a value that matches 6.*">
      <value operation="pattern match">^6\..*</value>
    </registry_state>
    <registry state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:2827" version="1"
      comment="The registry key has a value of Service Pack 2">
      <value>Service Pack 2</value>
    </registry_state>
    <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:3180" version="2">
      <value>amd64</value>
    </registry_state>
    <file_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:3185" version="2">
      <version operation="less than" datatype="version">6.0.2900.3164</version>
    </file_state>
    <file state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:3412" version="2">
      <version operation="less than" datatype="version">7.0.6000.20628</version>
    </file_state>
    <file state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:3490" version="2">
      <version operation="less than" datatype="version">6.0.3790.4106</version>
    </file_state>
    <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:3649" version="1" comment="x86 architecture">
      <value>x86</value>
    </registry_state>
    <file state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:org.mitre.oval:ste:394" version="1">
      <version datatype="version" operation="less than">6.1.0.9232</version>
    </file_state>
    <registry state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
      id="oval:gov.nist.fdcc.patch:ste:115263" version="0"
      comment="The registry key has a value of 5.1 or 5.2">
      <value operation="pattern match">5\.(1|2)</value>
```

```
    </registry_state>
  </states>
  <!-- ================================================================================ -->
  <!-- ================================  VARIABLES  ================================== -->
  <!-- ================================================================================ -->
  <variables>
    <local_variable id="oval:org.mitre.oval:var:206" version="1"
      comment="Windows common files\microsoft shared\triedit  directory" datatype="string">
      <concat>
        <object component item field="value" object ref="oval:org.mitre.oval:obj:281"/>
        <literal_component>\microsoft shared\triedit</literal_component>
      </concat>
    </local_variable>
    <local variable id="oval:org.mitre.oval:var:209" version="2"
      comment="Base path to vgx.dll, part of Vector Markup Language (VML) implementation."
      datatype="string">
      <concat>
        <object_component item_field="value" object_ref="oval:org.mitre.oval:obj:281"/>
        <literal_component>\Microsoft Shared\VGX</literal_component>
      </concat>
    </local_variable>
  </variables>
  <!-- ================================================================================ -->
  <!-- ================================================================================ -->
  <!-- ================================================================================ -->
</oval_definitions>
```

D.4 CPE Dictionary

This minimal CPE dictionary XML instance contains CPE Names referenced in the XCCDF document presented in section D.1.

Figure D-4. example-winxp-cpe-dictionary.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<cpe-list xmlns="http://cpe.mitre.org/dictionary/2.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://cpe.mitre.org/dictionary/2.0 http://cpe.mitre.org/files/cpe-
dictionary_2.1.xsd">
      <cpe-item name="cpe:/o:microsoft:windows xp">
            <title>Microsoft Windows XP</title>
            <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5" href="example-
winxp-cpe-oval.xml">oval:gov.nist.fdcc.xp:def:2</check>
      </cpe-item>
</cpe-list>
```

D.5 CPE Inventory

The following OVAL XML instance contains OVAL definitions that SHOULD be used to evaluate the CPE Name defined in the previous section.

Figure D-5. example-winxp-cpe-oval.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
                  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
                  xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5"
                  xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
                  xmlns:ind-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/windows-
definitions-schema.xsd
                  http://oval.mitre.org/XMLSchema/oval-definitions-5#independent
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/independent-
definitions-schema.xsd
                  http://oval.mitre.org/XMLSchema/oval-definitions-5
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/oval-
definitions-schema.xsd
                  http://oval.mitre.org/XMLSchema/oval-common-5
http://oval.mitre.org/language/download/schema/version5.3/ovaldefinition/complete/oval-common-
schema.xsd">
      <generator>
            <oval:product name>National Institute of Standards and Technology</oval:product name>
            <oval:schema_version>5.3</oval:schema_version>
            <oval:timestamp>2008-09-02T12:59:10.000-04:00</oval:timestamp>
      </generator>
      <!-- ================================================================================ -->
      <!-- ==============================  DEFINITIONS  ================================== -->
      <!-- ================================================================================ -->
      <definitions>
            <definition id="oval:gov.nist.fdcc.xp:def:2" version="1" class="inventory">
                  <metadata>
                        <title>Microsoft Windows XP is installed</title>
                        <affected family="windows">
                              <platform>Microsoft Windows XP</platform>
                        </affected>
                        <description>Microsoft Windows XP is installed</description>
                  </metadata>
                  <criteria>
                        <criterion comment="the installed operating system is part of the
Microsoft Windows family" test_ref="oval:gov.nist.fdcc.xp:tst:6"/>
                        <criterion comment="Microsoft Windows XP is installed"
test_ref="oval:gov.nist.fdcc.xp:tst:7"/>
                  </criteria>
            </definition>
      </definitions>
      <!-- ================================================================================ -->
      <!-- ================================  TESTS  ======================================= -->
      <!-- ================================================================================ -->
      <tests>
            <family_test id="oval:gov.nist.fdcc.xp:tst:6" version="1" comment="the installed
operating system is part of the Microsoft Windows family" check_existence="at least one exists"
check="only one" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent">
                  <object object_ref="oval:gov.nist.fdcc.xp:obj:3"/>
                  <state state_ref="oval:gov.nist.fdcc.xp:ste:14"/>
            </family_test>
            <registry_test id="oval:gov.nist.fdcc.xp:tst:7" version="1" comment="Microsoft
Windows XP is installed" check_existence="at least one exists" check="at least one"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
                  <object object_ref="oval:gov.nist.fdcc.xp:obj:4"/>
                  <state state_ref="oval:gov.nist.fdcc.xp:ste:15"/>
            </registry_test>
      </tests>
```

```
      <!-- ================================================================================ -->
      <!-- ================================  OBJECTS  ================================== -->
      <!-- ================================================================================ -->
      <objects>
            <family_object id="oval:gov.nist.fdcc.xp:obj:3" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"/>
            <registry_object id="oval:gov.nist.fdcc.xp:obj:4" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
                  <hive>HKEY_LOCAL_MACHINE</hive>
                  <key>SOFTWARE\Microsoft\Windows NT\CurrentVersion</key>
                  <name>CurrentVersion</name>
            </registry_object>
      </objects>
      <!-- ================================================================================ -->
      <!-- ================================  STATES  ================================== -->
      <!-- ================================================================================ -->
      <states>
            <family_state id="oval:gov.nist.fdcc.xp:ste:14" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent">
                  <family>windows</family>
            </family_state>
            <registry state id="oval:gov.nist.fdcc.xp:ste:15" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
                  <value>5.1</value>
            </registry state>
      </states>
      <!-- ================================================================================ -->
      <!-- ================================================================================ -->
      <!-- ================================================================================ -->
</oval_definitions>
```