



# **Improving FISMA Effectiveness and Efficiency Through the Security Content Automation Program (SCAP)**

**Shared Interest Group (SIG): Security and Privacy**

Date Released: January 28, 2008

The following White Paper addresses the challenges facing every federal agency with the cost and complexity of achieving FISMA security readiness and maintaining this readiness on a 24/7/365 basis. The National Institute of Standards and Technology (NIST), in cooperation with several FFRDCs, are defining the standards and interfaces for encoding information security information necessary to achieve, maintain and operationalize a high-level of information system security (ISS) readiness. This paper provides a roadmap to these standards and presents several models for a security architecture for enabling tools interoperability and pipelined solutions.

3040 Williams Drive - Suite 610 - Fairfax, VA 22031  
[www.actgov.org](http://www.actgov.org) - Phone: 703.208.4800 - Fax: 703.208.4805

*Leading the IT Community to Improve Government*

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

<b><i>American Council for Technology/Industry Advisory Council</i></b> _____	<b>3</b>
<b>Security and Privacy</b> _____	<b>3</b>
<b>Disclaimer</b> _____	<b>3</b>
<b>Copyright</b> _____	<b>4</b>
<b>Further Information</b> _____	<b>4</b>
<b><i>Purpose</i></b> _____	<b>5</b>
<b><i>Background</i></b> _____	<b>7</b>
<b><i>Discussion:</i></b> _____	<b>12</b>
<b>Best Practices</b> _____	<b>12</b>
<b>Information Security Systems (ISS) Line of Business</b> _____	<b>13</b>
<b><i>Analysis of Options:</i></b> _____	<b>15</b>
<b>Automation Standards</b> _____	<b>15</b>
Scope of Federal Security Related Standards _____	16
Security Content Automation Program (SCAP) _____	17
CVE and NVD _____	23
CCE _____	24
CPE _____	24
CVSS _____	25
Federal Desktop Core Configuration (FDCC) _____	26
<b>Application to FISMA Automation</b> _____	<b>26</b>
FISMA Compliance - Operational Scenario – How It All Comes Together _____	27
<b><i>Recommendations:</i></b> _____	<b>35</b>
<b><i>Impact Statement:</i></b> _____	<b>36</b>
<b><i>Author(s) &amp; Affiliations:</i></b> _____	<b>36</b>
<b><i>Bibliography</i></b> _____	<b>37</b>

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

## American Council for Technology/Industry Advisory Council

The American Council for Technology (ACT) is a non-profit educational organization established in 1979 to assist government in acquiring and using information technology resources effectively. In 1989 ACT established the Industry Advisory Council (IAC) to bring industry and government executives together to collaborate on IT issues of interest to the government. In 1997 ACT established the Intergovernmental Advisory Board (IAB) to foster communication and collaboration between IT executives at all levels of federal service – Federal, state, local and tribal governments.

The American Council for Technology, in cooperation with the Industry Advisory Council and Intergovernmental Advisory Board, is a unique, public-private partnership dedicated to helping government use technology to serve the public. The purposes of the organization are to communicate, educate, inform and collaborate. ACT also works to promote the profession of public IT management. ACT and IAC offer a wide range of programs to accomplish these purposes.

ACT and IAC welcome the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of information technology. For membership and other information, visit the ACT/IAC website at [www.actgov.org](http://www.actgov.org).

### **Security and Privacy**

The mission of the Information Security & Privacy Shared Interest Group is focused on bringing together the complementary challenges of both business areas. The goal is to provide thought leadership on ways to effectively provide the right level of security and privacy protection associated with the business responsibilities of an organization; as well as compliance with applicable governmental policy, regulations and laws.

### **Disclaimer**

This document has been prepared to provide information regarding a specific issue. This document does not – nor is it intended to – take a position on any specific course of action or proposal. This document does not – and is not intended to – endorse or recommend any specific technology, product or vendor. The views expressed in this document do not necessarily represent the official views of the individuals and organizations who participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT/IAC assumes no responsibility for consequences resulting from the use of the information herein.

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

**Copyright**

©American Council for Technology, 2008. This document may be quoted, reproduced and/or distributed without permission provided that credit is given to the American Council for Technology and Industry Advisory Council.

**Further Information**

For further information, contact the American Council for Technology and Industry Advisory Council at (703) 218-1955 or [www.actgov.org](http://www.actgov.org).

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

## Purpose

The information presented in this paper is targeted to the federal information security professional and industry partners responsible for achieving and maintaining a high-level of security readiness throughout the organization's information technology systems. The paper is designed to provide a foundation for the architecting of a comprehensive, enterprise-wide security automation solution with the goals of constantly improving security readiness and attainment of regulatory compliance in a cost efficient, practical manner.

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the E-Government Act of 2002 (Pub. L. No. 107-347). The goals of FISMA include development of a comprehensive framework to protect the government's information, operations, and assets. Providing adequate security for the Federal government's investment in information technology (IT) is a significant undertaking. In fiscal year 2006, the Federal agencies spent \$5.5 billion securing the government's total IT investment of approximately \$63 billion equating to approximately 9 percent of the total IT portfolio. As described in Chapter III, these funds were used for a variety of security programs including certification and accreditation of systems, testing of controls, and user awareness training.

FISMA assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen IT system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information security risks to an acceptable level.

To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB. OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with FISMA.

To ensure the safeguard of personally identifiable information (PII), agencies are also required to report on several performance metrics related to information privacy. In addition to tracking the metrics required by the E-Government Act, agencies are also required to report on several additional metrics, including those required by the Privacy Act (5 U.S.C. § 552a), which OMB is charged with implementing.

To "get to green" under the E-Government Scorecard, agencies must meet the following three security criteria:

- IG or Agency Head verifies the effectiveness of the Department-wide IT security remediation process;
- IG or Agency Head rates the agency certification and accreditation process as "Satisfactory" or better; and
- The agency has 90 percent of all IT systems properly secured (certified and accredited).

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

In order to “maintain green,” by July 1, 2007, agencies needed to meet the following security and privacy criteria:

- All systems certified and accredited;
- Systems installed and maintained in accordance with security configurations;
- Has demonstrated for 90 percent of applicable systems a Privacy Impact Assessment (PIA) has been conducted and is publicly posted; and

Has demonstrated for 90 percent of systems with PII contained in a system of records covered by the Privacy Act to have developed, published, and maintained a current SORN.

*From a technology perspective, security assessment standardization work is being done at NIST that is designed to move the industry, methodologies and tools toward uniform modeling of security related concepts, data and interfaces. This work is the primary subject matter of this paper. This paper presents an overview of this work and describes how it can be applied to an enterprise-wide security management platform bringing together best-in-class processes and technology with the goal of reducing the overall cost, while increasing the efficiency and effectiveness, of the FISMA, E-Government Act, Privacy Act, OMB policy, and NIST guidelines compliance process. This paper covers 6 of these security related specifications within the context of achieving FISMA compliance. Many more specifications can be found at [Making Security Measurable](#).*

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

## Background

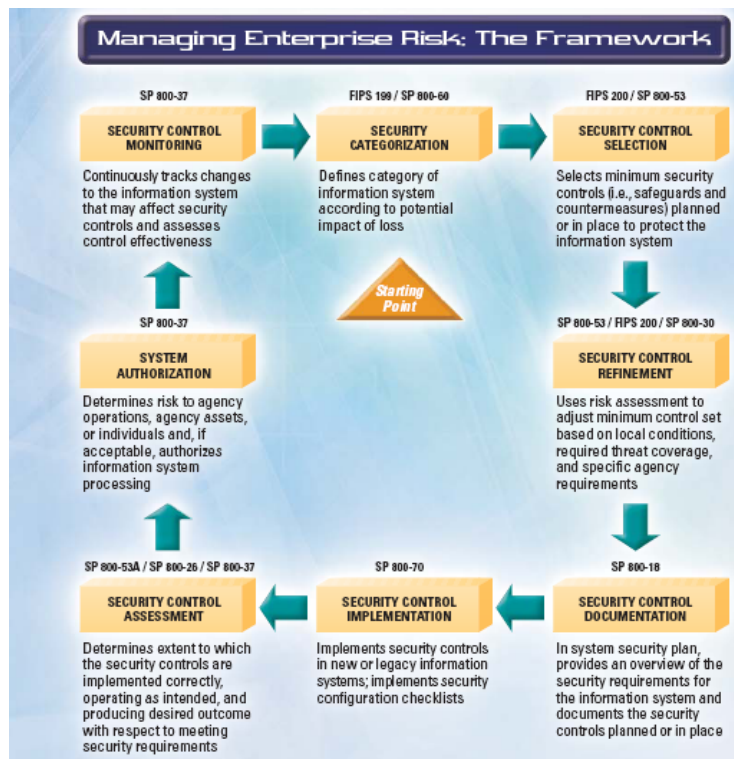
The challenges facing federal agency information technology staff, when compared to their commercial industry counterparts, are significant given the level of external oversight that exists ranging from the internal inspector general (IG) to the OMB and Congressional committees.

The Federal Information Security Management Act (FISMA) was enacted in December 2002 and the inherent requirements for periodic Certification and Accreditation (C&A) projects has increased the demand for tools to improve the productivity of the IT teams performing this work.

Another key challenge presented by FISMA compliance is the evolving and changing nature of the underlying IT infrastructure. Changes to the infrastructure occur constantly thereby making any C&A results a snapshot of the state of the assets at the time the evaluation was performed. The objective of C&A is to initially certify and accreditate the systems, and then to continuously monitor and report the level of compliance over time. Since it is impractical to constantly C&A an IT asset, there is a need for compliance automation that supports the operational and maintenance environment that exists today; this requires solutions that provide constant monitoring of changes such as router reconfiguration, server operating system patches and the addition of new accounts in the network directory.

Figure 1 provides an view of the life-cycle for risk assessment with references to regulatory references and applicable NIST documentation. The focus of the NIST work on security data modeling is focused on the Security Control Implementation and Security Control Assessment steps in this life-cycle.

**Figure 1: Security Risk Life-Cycle**

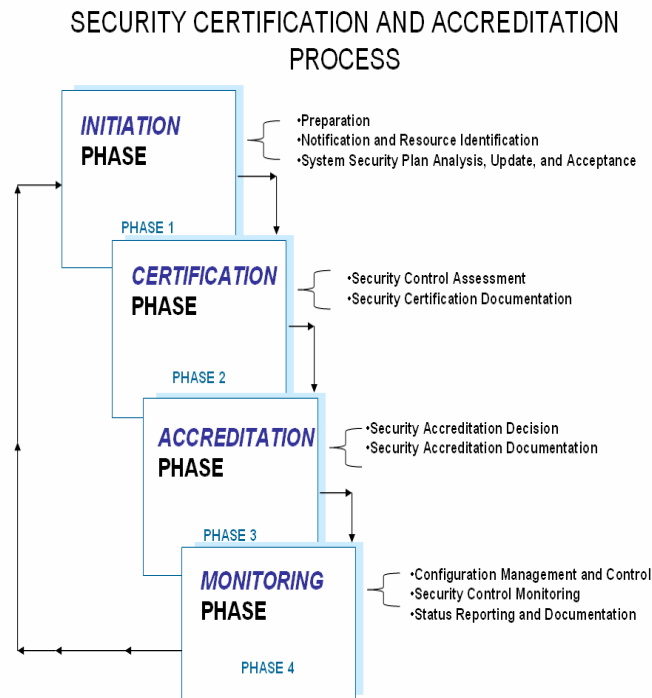


## Improving FISMA Effectiveness and Efficiency Through the Security Content Automation Program (SCAP)

The primary objective of this paper is to orient the reader to the potential benefits of automation at the various stages of compliance evaluation methods as defined by industry best practice and consistent with the National Institute of Standards and Technology (NIST) security certification and accreditation process guidance, (NIST Special Publication 800-37-Guide for the Security Certification and Accreditation of Federal Information Systems), which consists of the following distinct phases:

- Initiation Phase;
- Security Certification Phase;
- Security Accreditation Phase; and
- Continuous Monitoring Phase.

**Figure 2: Security Certification and Accreditation**



FISMA and OMB policy requires agencies to test system security controls annually. In fiscal year 2006, agencies tested security controls for 88 percent of systems and contingency plans for 77 percent of all systems, up from 61 percent and 72 percent respectively in fiscal year 2005. The Department of Defense (DOD) alone increased system testing by more than 30 percent from 2005 to 2006. Though rates of testing for system security controls and contingency plans increased, that improvement is largely attributable to moderate and low risk systems, as well as uncategorized systems. The percentage of uncategorized systems with

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

tested security controls climbed from 42 percent to 93 percent. OMB continues to track this metric quarterly, by risk impact level, and uses this metric as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.<sup>i</sup>

IGs reported the overall quality of the certification and accreditation (C&A) processes at agencies decreased from 17 to 16 of the 25 agencies having a process in place rated as "satisfactory" or better. Eight agencies had C&A processes rated as "good" or "excellent," an increase from 5 in fiscal year 2005. Nine IGs reported overall C&A processes as "poor" or "failing," an increase of 1 from fiscal year 2005. This is an overall decrease in IG ratings from 2005, where 17 agencies were reported as "satisfactory" or better, yet the number of agencies moving to the "good" and "excellent" categories increased in 2006.<sup>ii</sup>

OMB asked IGs to confirm whether the agency ensures information systems used or **operated by a contractor** of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines. The majority (18 of 24) of agency IGs categorized the extent of agency's oversight as "frequently" (2 agencies), "mostly" (1 agency), and "almost always" (15 agencies); however, several (6 of 24) agency IGs rate the extent of agency oversight as "rarely" (3 agencies) or "sometimes" (3 agencies).<sup>iii</sup>

**Table 1: Agency Reported C&A Process Quality**

Rating	Qty(agencies)	%
Excellent	2	8%
Good	6	24%
Satisfacto	8	32%
Poor	8	32%
Failing	1	4%
Total	25	

Now consider if NIST, with the support of OMB, provided common test procedures that included low-level system checks that enabled automation of the security control assessment and monitoring activities. Significant benefits would be captured if NIST provided this content not as another Special Publication, but as an open, standards-based XML data streams that included requirements traceability to the information assurance control references in SP 800-53 required for reporting. Repurposable data and ease of integration would result when the vendor community supports security and systems management and embraces these standard data exchange methods and common enumeration schemes that enable semantic knowledge to be embedded within the data exchange.

This would provide an opportunity to improve the quality of the C&A processes, enable an agencies' ability to streamline, automate, and reduce the cost of the overall C&A process, and ultimately improve an agencies' actual security posture.

### **What are the Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP)**

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

The Information Security Automation Program (ISAP) is a U.S. government multi-agency initiative to enable automation and standardization of technical security operations. The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). The NIST [National Vulnerability Database \(NVD\)](#) is the U.S. government content repository for ISAP and SCAP.

One of the primary goals of the SCAP is to encourage the development of checklists in XML formats, particularly checklists that are compliant with Extensible Configuration Checklist Description Format (XCCDF) and/or Open Vulnerability and Assessment Language (OVAL). This section first provides a high-level overview of XCCDF and/or OVAL, and explains how they can be used for checklists. It then focuses on the use of XCCDF and/or OVAL-compliant checklists for helping agencies with FISMA compliance efforts, and also compares the FISMA and DOD 8500.2/8510 compliance efforts.

A security checklist is a document that contains instructions for securely configuring an information technology (IT) product for an operational environment or verifying that an IT product has already been securely configured. Checklists can take many forms, including files that can automatically set or verify security configurations; having such automated methods has become increasingly important for several reasons, including the complexity of achieving compliance with various laws, regulations, and guidelines, and the increasing rates of vulnerabilities in systems and threats against those vulnerabilities. Automation is also needed to ensure that systems are secured consistently and their security verified effectively.<sup>iv</sup>

Implementing SCAP standards in peripheral disciplines like asset and configuration management is not mandatory when using SCAP to standardize and automate security operations. However, implementing the enumeration standards Common Configuration Enumeration (CCE) within configuration management practices and Common Platform Enumeration (CPE) within asset management practices will partially standardize those practices, set the stage for automation, including automation across products of various manufacture, and enable interoperability at the interfaces between your configuration, asset, vulnerability, and compliance management practices. The net effect is more efficiency throughout IT programs and forwarding the vision of baking security into IT. As a first step toward obtaining these benefits, the recommendation is to initiate dialog with your configuration and asset management vendors with regards to their plan for implementing applicable SCAP standards and automating interfaces with products and services that exist in the vulnerability and compliance management domains.

### **Problem Statement**

Throughout many departments and agencies, the operational security management plus Certification and Accreditation processes are very costly and limited in effectiveness due to:

- Manual, disjointed and inconsistent processes for information technology (IT) asset discovery, assessment and monitoring increase the cost and introduce errors in reporting that result in inadequate remediation. Solution - Standards for best practices are needed to improve consistency and accountability across platforms, offices, agencies and departments.

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

- Manual or disjointed automation requiring a substantial amount of manpower to perform assessments and tests. Solution – Better design and integration of tools are needed to reduce the labor and increase the quality/consistency of asset discovery, assessment (e.g. configuration), testing and results reporting.
- Inconsistent and inaccurate terminology is being used to identify and define security problems. Solution – Define standard terminology dictionaries that are both human and machine understandable/readable.
- Systems and networks are only periodically tested (every 1 to 3 years) leaving assets vulnerable to interim attacks due to addition/removal of IT systems, design changes and misconfiguration. Solution – Provide near-real-time, constant monitoring of assets and create administrator alerts to system changes that deviate from the FISMA compliant or secured states.

### **Solution**

From a management perspective, the current Administration intends to focus on the implementation of the Information Systems Security (ISS) line of business (LOB) to increase security effectiveness and reduce costs across government. The establishment of shared service centers for security training and FISMA reporting is the first step towards ensuring greater use of standardized products and services.

OMB has integrated IT security and privacy into the capital planning and investment control process to promote greater attention to security and privacy as fundamental management priorities. To guide agency resource decisions and assist OMB oversight, OMB Circular A-11, “Preparation, Submission and Execution of the Budget,” requires agencies to:

- Report security costs for all IT investments;
- Document adequate security controls and costs have been incorporated into the life cycle planning of each investment; and
- Tie the POA&Ms for a system directly to the funding request for the system.

Part 7 (Exhibit 300) of OMB Circular A-11 requires agencies to submit a Capital Asset Plan and Business Case justification for major IT investments. **In their justification, agencies must answer a series of security and privacy questions and describe how the investment meets the requirements of the FISMA, E-Government Act, Privacy Act, OMB policy, and NIST guidelines.** The justifications are then evaluated on specific criteria including whether the system’s cyber-security, planned or in place, is appropriate.<sup>v</sup>

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

Discussion:

**Best Practices**

Best practices is a reference to the assertion that there is a technique, method, process, activity, incentive or reward that is more effective at delivering a particular outcome than any other technique, method, process, etc. The idea is that with proper processes and methods, which have been tested and validated by a broad cross section of industry, a desired outcome can be delivered with fewer problems and unforeseen complications. Best practices may also be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of organizations.

One example of a Best Practices repository is the National Institute of Standards and Technology (NIST) sponsored “security checklist” program that represents Best Practice from the perspective of the submitters (often the vendor of the product) with NIST oversight. This responsibility is derived from the [Cyber Security Research and Development Act](#) which requires NIST to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that, or is likely to become widely used, within the Federal Government.

The first iteration of this initiative was the NIST Checklist Program. More specifically, NIST, with sponsorship from the Department of Homeland Security (DHS), has produced Special Publication 800-70: Security Configuration Checklists Program for IT Products - Guidance for Checklist Users and Developers to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products.

How does this help agencies with compliance from FISMA-related perspective?

FISMA (section 3544(b)(2)(D)(iii)) requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. Accordingly, Federal agencies, as well as vendors of products for the Federal government, are encouraged to acquire or develop and share such checklists using the NIST repository. The development and sharing of these checklists can greatly reduce what would otherwise be a “reinvention of the wheel” for IT products that are widely used in the Federal government, e.g., common operating systems and office applications.

The program has since evolved from the representation of security configuration best practices in human readable documents (i.e. word, pdf, etc) designed for technicians to XML based documents that can be transformed to be read by human, or more importantly, to be machine readable for an automated system to assess and score a systems conformance to the information detailed in the XML.

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)  
**Information Security Systems (ISS) Line of Business**

The [Information Systems Security Line of Business \(ISS LOB\)](#) is an interagency effort to identify ways to make consistent and strengthen the ability of all agencies to identify and defend against threats, correct vulnerabilities, and manage risks. DHS serves as the managing agency for this line of business, which is part of the President's E-Government Initiatives.

The ISS LOB selected three agencies as shared service centers for security awareness training; 1) DOD, 2) the Office of Personnel Management, and 3) DOS – in coordination with the United States Agency for International Development. Additionally, two agencies were selected as shared service centers for FISMA reporting; 1) the Department of Justice and 2) the Environmental Protection Agency. These agencies were selected through a competitive and analytically-derived process based on their qualifications and ability to provide information security products and services on a government-wide basis. Each shared service center has a business process in place to support cross-agency servicing, and agencies will now select their center and provide the ISS LOB with their plans to migrate to them. Shared service centers for security awareness training and FISMA reporting began operation in April 2007.

Shared service centers will eliminate the need for each agency to develop security awareness training or obtain an automated tool for managing their FISMA reporting on their own. This will maximize resources and result in standardized information security programs and better-trained workforces, cognizant of their information security responsibilities. It will also allow agencies to dedicate their limited resources to critical, mission-specific security issues. By providing shared solutions for common information security areas, the ISS LOB will allow all federal departments and agencies to benefit from improved levels of cyber security, reduced costs, elimination of duplicative efforts, and improved quality of service and expertise through specialization and consolidation.<sup>vi</sup>

The agencies providing FISMA reporting services have a GOTS (Government Off The Shelf) software solution “purpose built” for FISMA reporting. This includes the [DOJ Cyber Security Assessment and Management \(CSAM\)](#) solution and the EPA [Automated Security Self-Evaluation and Remediation Tracking \(ASSERT\)](#) solution. These solutions have initiatives underway to incorporate NIST SCAP results for the IA controls that can be automatically tested via NIST SCAP based solutions, eliminating the error prone manual data entry exercise for representing a systems adherence to the FISMA policies for security configurations and risk assessments.

With CSAM, program offices can manage their Risk-Based Policy & Implementation Guidance, more specifically by documenting:

- Threats and Vulnerabilities
- Roles – Responsibilities - Privileges
- Standards

through online electronic data capture.

With ASSERT, program offices can create a Plan of Action and Milestones (POA&M) when it identifies a security control weakness. The POA&M, which documents the planned remediation process, is recorded in the Agency's Automated Security Self-Evaluation and

## Improving FISMA Effectiveness and Efficiency

Through the Security Content Automation Program (SCAP)

Remediation Tracking (ASSERT) tool. ASSERT is used to centrally track remediation of weaknesses associated with information systems and can serve as the Agency's official record for POA&M activity.

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

**Analysis of Options:**

Historically, the accepted methods for assessing FISMA security have consisted of:

- Periodic (every 3 years) Certification and Accreditation (C&A) projects following agency specific guidelines and procedures (e.g. NIACAP for Civilian, DITSCAP/DIACAP for Military);
- Use of discrete, non-integrated, standalone tools ranging from asset/network discovery to configuration testing to vulnerability testing;
- Manually created reports documenting the assets to be tested, test procedures, expected results, test results and remediation recommendations.

Examples of the kinds of problems resulting from these methods includes:

- Inconsistent documentation from system to system (as well as within a given system) creating misunderstandings, errors and an inability to compare longitudinal results;
- Costly, repetitive manual processes;
- Vulnerabilities between testing periods created by changes to the assets (e.g. computers, software, network devices).
- Lack of objective testing and results that properly assessed the state of the assets.

What is needed are human and machine readable standards that would improve the accuracy of the tests and results as well as enable the automation of repetitive, manual procedures for testing and documentation.

**Automation Standards**

This section presents an overview of a key subset of the SCAP and related standards that can be applied to various categories of security measurement tools to support standardized encoding of information and interfaces (the data model).

The benefits of using these standards include:

- Pipelining of tools for an integrated solution to information security management;
- Repurposing of data from tools for discovery, data mining and archival;
- Logitudinal comparisons of data for constant monitoring of security readiness;
- Interoperability of tools through exchanged data (e.g. non-pipelined);
- Interchangeable tool swap-out or replacement for upgrading or competitive sourcing.

Through security standards, compliance and certification of vendor products, an agency can ensure that a comprehensive security compliance system with constant monitoring can be architected from interchangeable components using “best-in-class” technologies. An added benefit is the ability to “plug-n-play” various security tool components enabling selective upgrading or expansion in accordance with information systems requirements (e.g. capital budgets for continuous security improvement).

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

## Scope of Federal Security Related Standards

Various security standards that can be used for automation of various security management related tasks can be found at [Making Security Measurable](#). A brief introduction to each of these standards is presented below.

### Enumerations

- Common Vulnerabilities and Exposures (CVE®) - common vulnerability identifiers
- Common Weakness Enumeration (CWE™) - list of software weakness types
- Common Attack Pattern Enumeration and Classification (CAPEC™) - list of common attack patterns
- Common Malware Enumeration (CME™) - common identifiers for viruses, worms, and other malicious code
- Common Configuration Enumeration (CCE™) - common security configuration identifiers
- Common Platform Enumeration (CPE™) - common platform identifiers
- SANS Top Twenty - SANS/FBI consensus list of the Twenty Most Critical Internet Security Vulnerabilities that uses CVE-IDs to identify the issues
- OWASP Top Ten - ten most critical Web application security flaws

### Languages

- WASC Web Security Threat Classification - list of Web security threats
- Open Vulnerability and Assessment Language (OVAL™) - standard for determining vulnerability and configuration issues
- Extensible Configuration Checklist Description Format (XCCDF) - specification language for uniform expression of security checklists, benchmarks, and other configuration guidance
- Common Vulnerability Scoring System (CVSS) - open standard that conveys vulnerability severity and helps determine urgency and priority of response
- Common Announcement Interchange Format (CAIF) - XML-based format created to store and exchange security announcements in a normalized way
- OMG Semantics of Business Vocabulary and Business Rules (SBVR) - language for interchange of business vocabularies and rules among organizations and software tools

### Repositories

- OVAL Repository - community-developed OVAL Vulnerability, Compliance, Inventory, and Patch Definitions

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

- National Vulnerability Database (NVD) - U.S. vulnerability database based on CVE that integrates all publicly available vulnerability resources and references
- NIST Security Content Automation Protocol (SCAP) - security content for automating technical control compliance activities, vulnerability checking, and security measurement
- Red Hat Repository - OVAL Patch Definitions corresponding to Red Hat Errata security advisories
- Center for Internet Security (CIS) Benchmarks - best-practice consensus bases security configurations accepted for compliance with FISMA, the ISO standard, GLB, SOx, HIPAA, and FIRPA, and other regulatory requirements for information security
- DISA Security Technical Implementation Guides (STIGS) - U.S. Defense Information Systems Agency's (DISA) STIGS are configuration standards for DOD information assurance and information assurance-enabled devices and systems

NIST has a Security Configuration Checklists Repository available for public use at <http://checklists.nist.gov/>. The repository contains checklists that have been developed and screened to meet the requirements of the NIST Security Configuration Checklists Program for IT Products, which is the predecessor to the new National Checklist Program. As of mid-2006, the beta version of the repository hosted over 115 checklists addressing over 155 specific IT products. The format of the checklists varies widely, from documents written in English prose to files and scripts written for use with automated tools. An example of such a tool is the DISA Gold Disk, which can scan a system for configuration settings that differ from policy requirements.

### **Security Content Automation Program (SCAP)**

This paper focuses on the subset of standards that are encapsulated within the Security Content Automation Program (SCAP). In response to these needs, the SCAP seeks to encourage the development of automated checklists, particularly those that are compliant or compatible with the Extensible Configuration Checklist Description Format (XCCDF) and/or the Open Vulnerability and Assessment Language (OVAL). These are widely used for automated checklists—XCCDF primarily for mapping regulatory policies and other sets of requirements to high-level technical rules, and OVAL primarily for mapping high-level technical rules to the low-level details of executing those checks. For example, XCCDF could map a requirement for authentication management in NIST Special Publication (SP) 800-53 to a specified need to check that the system's minimum password length is at least 8 characters. OVAL could then define how that check should be performed on a particular type of system, such as a Windows computer or a UNIX computer.<sup>vii</sup>

SCAP is a suite of selected open standards that enumerate software flaws, security related configuration issues, and product names; measure systems to determine the presence of vulnerabilities; and provide mechanisms to rank (score) the results of these measurements in order to evaluate the impact of the discovered security issues. SCAP defines how these standards are combined. The National Vulnerability Database provides a repository and data

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

feeds of content that utilize the SCAP standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance).

Recently, NIST has encapsulated six (6) different standards initiatives through the SCAP initiative as shown in the [National Vulnerability Database](#). As recently as 2006, only the XCCDF and OVAL specifications were considered a part of SCAP. Now the following additional standards have been included:

- Common Vulnerabilities and Exposures ([CVE](#))
- Common Configuration Enumeration ([CCE](#))
- Common Platform Enumeration ([CPE](#))
- Common Vulnerability Scoring System ([CVSS](#))




Security content automation is the process of using tools, scripts, and other technologies to automate the application or verification of security-related configuration settings for operating systems and applications, as specified in XCCDF and/or OVAL-compliant or compatible checklists. SCAP leverages separate but complementary government efforts as part of its integrated solution for security content automation. The primary intentions of the SCAP is to improve the application, verification, and reporting of security configuration settings.

SCAP specifically focuses on the creation of checklists that support agency compliance with FISMA and map to the minimum security controls for information systems described in NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, and the information system categories described in Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.<sup>viii</sup>




These six (6) SCAP open standards are summarized in Table 2. The purpose of each standard is shown in Table 3. This suite of standards is expected to grow over time to address emerging issues that face the vulnerability management and security compliance community.

The U.S. National Institute of Standards and Technology (NIST) defines and maintains the protocol and the data feeds of content in the SCAP standards. Thus, NIST defines how to use the open standards within the SCAP context and defines the mappings between the SCAP enumeration standards. However, NIST does not control the underlying standards that are used within the protocol. Table 2: SCAP Standards Overview provides brief definitions of each of these standards.







**Table 2: SCAP Standards Overview**

	Common Vulnerabilities and Exposures	Standard identifiers and dictionary for security vulnerabilities related to software flaws
	Common Configuration Enumeration	Standard identifiers and dictionary for system configuration issues related to security
	Common Platform Enumeration	Standard identifiers and dictionary for platform/product naming

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

	eXtensible Configuration Checklist Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
	Open Vulnerability and Assessment Language	Standard XML for testing procedures for security related software flaws, configuration issues, and patches as well as for reporting the results of the tests
	Common Vulnerability Scoring System	Standard for conveying and scoring the impact of vulnerabilities

**Table 3: SCAP Suite of Open Standards Coverage Map**

	Enumeration	Evaluation	Measuring	Reporting	Content
	√				√
	√				√
	√				√
		√		√	√
		√		√	√
			√		√

The document [The Security Content Automation Program, NIST IR-7343 \(Draft\)](#) provides an overview of only the XCCDF and OVAL components of SCAP, and then examines how security content automation can be beneficial in achieving compliance with the Federal Information Security Management Act (FISMA), the Department of Defense (DOD) 8500.2/8510, and other compliance requirements. It also provides details on how SCAP utilizes vulnerability checking and compliance standards within its implementation: the Extensible Configuration Checklist Description Format (XCCDF) and the Open Vulnerability Assessment Language (OVAL). Many of the concepts discussed in this document can be extended to the other four (4) standards recently organized under the SCAP.

These SCAP specifications have many useful application in securing the governments information technology assets as described below.

**Secure Configurations**

Agencies and other organizations could consistently monitor their operating systems and applications, using SCAP tools and content, to ensure that they maintain a secure

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

configuration. Such tools can also assist with automating implementation of an initial secure configuration for new assets (secure images may also be used for this purpose in some cases). Within the U.S. government, SCAP should be used to ensure that operating systems and applications conform to NIST security configuration guidance. The DOD also publishes SCAP content and DOD profiles are often available within NIST SCAP content.

### **FISMA Technical Control Compliance Automation**

Agencies and other organizations can automate much of their FISMA technical security control compliance activities by regularly scanning information technology assets using SCAP checklists. SCAP checklists have FISMA compliance mappings embedded within the checklist so that SCAP-compatible tools can automatically generate NIST Special Publication 800-53 assessment and compliance evidence. Each low level security configuration check is mapped to the appropriate high level NIST SP 800-53 security controls. In addition, the SCAP checklists also contain mappings to other high level policies (e.g., ISO, DOD 8500, FISCAM) and SCAP tools may also output those compliance mappings.

### **Customization of Recommended Secure Configurations**

Agencies and other organizations can customize recommended SCAP secure configurations (e.g., NIST checklists) to tailor them to specific environments. SCAP checklists, being represented in standards based XML formats, are an ideal format for customization. Organizations can modify checks, delete checks, add new checks, and digitally sign their changes. Then SCAP compatible tools will be able to automatically process the customized checklists (without any additional coding being required or even any involvement from the SCAP tool vendor).

### **Integration and Automation of Security Operations**

Agencies and other organizations can integrate and automate disjoint security operations activities and databases through adoption of SCAP. This can be achieved by integrating vulnerability databases, incident databases, intrusion detection databases, and asset databases using SCAP data as primary keying material. For example, all security products and databases should use standard names for software flaws, configuration issues, and product names.

### **Communications Involving Vulnerabilities**

Agencies and other organizations can use SCAP vulnerability and product naming enumeration standards when communicating about vulnerabilities (security related software flaws and misconfigurations). Agencies and other organizations can report incident details (both internally and externally) using SCAP vulnerability and product names to the greatest extent possible. This ensures that all vulnerability communications precisely identify the relevant low level issues, enable integration of data feeds using this same standardized language, and enable easy correlation with other data repositories that may have additional information on the relevant vulnerabilities.

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

The Security Content Automation Program (SCAP) seeks to encourage the development of automated checklists, particularly those that are compliant or compatible with the Extensible Configuration Checklist Description Format (XCCDF) and/or the Open Vulnerability and Assessment Language (OVAL). These are widely used for automated checklists—XCCDF primarily for mapping policies and other sets of requirements to high-level technical checks, and OVAL primarily for mapping high-level technical checks to the low-level details of executing those checks. For example, XCCDF could map a requirement for authentication management in NIST Special Publication (SP) 800-53 to a specified need to check that the system's minimum password length is at least 8 characters. OVAL could then define how that check should be performed on a particular type of system, such as a Windows computer or a UNIX computer.

### **XCCDF**

[Extensible Configuration Checklist Description Format \(XCCDF\)](#) from the NSA's National Vulnerability Database is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. 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 foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices. Development of the XCCDF specification is being led by NSA, with contributions from other agencies and organizations.

[XCCDF 1.1.3](#) is designed to enable easier, more uniform creation of security checklists and procedural documents, and allow them to be used with a variety of commercial, Government off-the-shelf (GOTS), and open source tools. The motivation for this is improvement of security for IT systems, including the Internet, by better application of known security practices and configuration settings.

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.

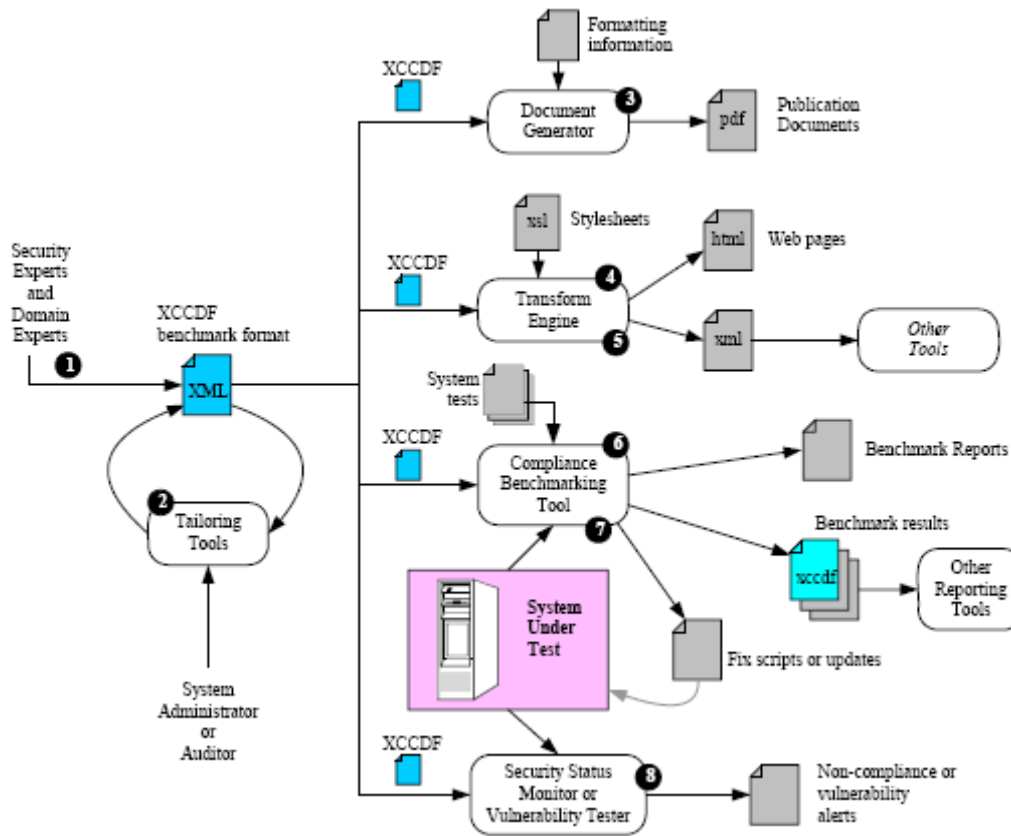
XCCDF is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. 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 foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices.

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

One potential use for XCCDF is streamlining compliance to FISMA and Department of Defense (DOD) STIGs. XCCDF proposes to automate certain technical aspects of security by converting English text contained in various publications (e.g., configuration guides, checklists, the National Vulnerability Database [NVD]) into a machine-readable XML format such that the various audiences (e.g., scanning vendors, checklist/configuration guide, auditors) will be operating in the same semantic context. The end result will allow organizations to use commercial off-the-shelf (COTS) tools to automatically check their security and map to technical compliance requirement. Other possible Use Cases for application of the standard are shown in Figure 3.

**Figure 3: Use Cases for XCCDF Document<sup>ix</sup>**



## OVAL

OVAL is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. The OVAL Language is a collection of XML schema for representing system information, expressing specific machine states, and reporting the results of an assessment. The OVAL repository is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions.

Open Vulnerability and Assessment Language (OVAL) is used to specify the technical details for checking systems for the presence of vulnerabilities and configuration issues. A set of

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

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.

OVAL definitions are standardized, machine-readable tests written in the [Open Vulnerability and Assessment Language \(OVAL™\)](#) that check the machine state of computer systems for the presence of software vulnerabilities, configuration issues, programs, and patches. OVAL definitions, which are free to use and implement in information security products and services, are written in Extensible Mark-up Language (XML) and are available for most major platforms.

There are four types of OVAL definitions:<sup>x</sup>

- 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”.

## CVE and NVD

The Common Vulnerabilities and Exposures (CVE) vulnerability naming standard is a dictionary of names for most publicly known security flaws in IT software. The CVE industry standard has achieved wide acceptance by the security industry and a number of government organizations. It is funded by US-CERT and the technical analysis work is done at MITRE Corporation. General CVE information is available at <http://cve.mitre.org/>.

CVE provides the computer security community with the following:

- A comprehensive list of publicly known vulnerabilities
- An analysis of the authenticity of newly published vulnerabilities
- A unique name to be used for each vulnerability.

The vulnerabilities listed in CVE can be best viewed using the National Vulnerability Database (NVD), which provides summaries for all CVE vulnerabilities. Each summary contains attributes of the vulnerability (including a short summary and vulnerable version numbers) and links to advisories, patches, and other resources related to the vulnerability. NVD offers a fine-grained search engine that allows users to search for vulnerabilities containing a variety of characteristics. For example, users can search on product characteristics such as vendor name, product name, and version number, or on vulnerability characteristics such as severity, related exploited range, and type of vulnerability. NVD also supports queries in OVAL format. NVD is available at <http://nvd.nist.gov/>.

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

CVE has not been adopted by any formal standards body. It is a widely used self-declared standard. NIST SP 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, is available at <http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf>.

Any product containing NVD or CVE data can be integrated with the NVD web site vulnerability summaries. To link to a particular vulnerability summary, simply use the hyperlink format <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2001-0322> where "CVE-2001-0322" is replaced with the name of the vulnerability of interest.

## CCE

In mid-2006, plans for a Common Configuration Enumeration (CCE) standard were announced. It is very similar to CVE, but it addresses security misconfigurations in software deployments instead of flaws with the software itself. Checklists could refer to CCE names for misconfigurations just as they refer to CVE names for software flaws. More information on CCE is available at <http://cve.mitre.org/cce/>.<sup>xi</sup>

CVE is widely used in tools and repositories such as:

### Tool

- Vulnerability Management
- Patch Management
- Vulnerability Alerting
- Intrusion Detection

### Repository

- NVD (National Vulnerability Database)
- US-CERT Bulletins
- SANS Top 20

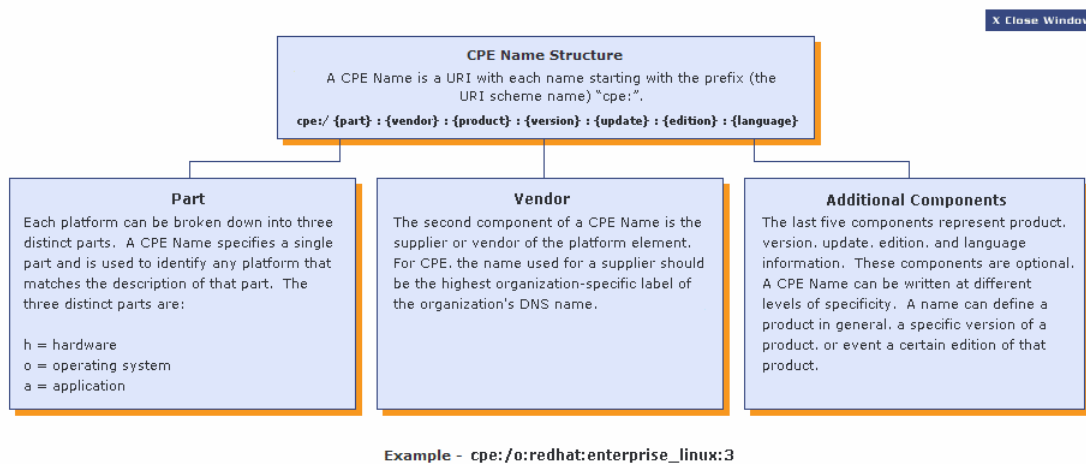
## CPE

[CPE™](#) is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

The power of the CPE standard is in the uniformity in defining a particular component of the IT system that can then be linked to recommended configuration data defined in CCE and security vulnerabilities defined in CVE. This uniformity and name structure (as shown in Figure 4) enable extensive automation as described in Section 0 Application to FISMA.

# Improving FISMA Effectiveness and Efficiency Through the Security Content Automation Program (SCAP)

Figure 4: CPE [Name Structure](#)



## CVSS

The [Common Vulnerability Scoring System \(CVSS\)](#) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

In particular, NVD supports the Common Vulnerability Scoring System (CVSS) version 2 standard for all CVE vulnerabilities. NVD provides CVSS 'base scores' which represent the innate characteristics of each vulnerability. We do not currently provide 'temporal scores' (scores that change over time due to events external to the vulnerability). However, NVD does provide a [CVSS score calculator](#) to allow you to add temporal data and to even calculate environmental scores (scores customized to reflect the impact of the vulnerability on your organization). This calculator contains support for U.S. government agencies to customize vulnerability impact scores based on FIPS 199 System ratings. An [expert version of this calculator](#) is also provided by the NVD.

Many organizations are using CVSS, and each are finding value in different ways. Below are some examples:<sup>xii</sup>

- **Vulnerability Bulletin Providers:** Both non-profit and commercial organizations are publishing CVSS base and temporal scores and vectors in their free vulnerability bulletins. These bulletins offer much information, including the date of discovery, systems affected and links to vendors for patching recommendations.

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

- **Software Application Vendors:** Software application vendors are providing CVSS base scores and vectors to their customers. This helps them properly communicate the severity of vulnerabilities in their products and helps their customers effectively manage their IT risk.
- **User Organizations:** Many private-sector organizations are using CVSS internally to make informed vulnerability management decisions. They use scanners or monitoring technologies to first locate host and application vulnerabilities. They combine this data with CVSS base, temporal and environmental scores to obtain more contextual risk information and remediate those vulnerabilities that pose the greatest risk to their systems.
- **Vulnerability Scanning and Management:** Vulnerability management organizations scan networks for IT vulnerabilities. They provide CVSS base scores for every vulnerability on each host. User organizations use this critical data stream to more effectively manage their IT infrastructures by reducing outages and protecting against malicious and accidental IT threats.
- **Security (Risk) Management:** Security Risk Management firms use CVSS scores as input to calculating an organization's risk or threat level. These firms use sophisticated applications that often integrate with an organization's network topology, vulnerability data, and asset database to provide their customers with a more informed perspective of their risk level.
- **Researchers:** The open framework of CVSS enables researchers to perform statistical analysis on vulnerabilities and vulnerability properties.

### **Federal Desktop Core Configuration (FDCC)**

The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FDCC currently exists for Microsoft Windows Vista and XP operating system software. While not addressed specifically as the "Federal Desktop Core Configuration," the FDCC was originally called for in a 22 March 2007 memorandum from OMB to all Federal agencies and department heads and a corresponding memorandum from OMB to all Federal agency and department Chief Information Officers (CIO).

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

### **Application to FISMA Automation**

As astute Federal CIOs and Chief Information Security Officers know, establishing compliance to the FISMA regulations and maintaining that compliance is a complex and expensive undertaking. A Recent OMB report indicated that In fiscal year 2006, the Federal

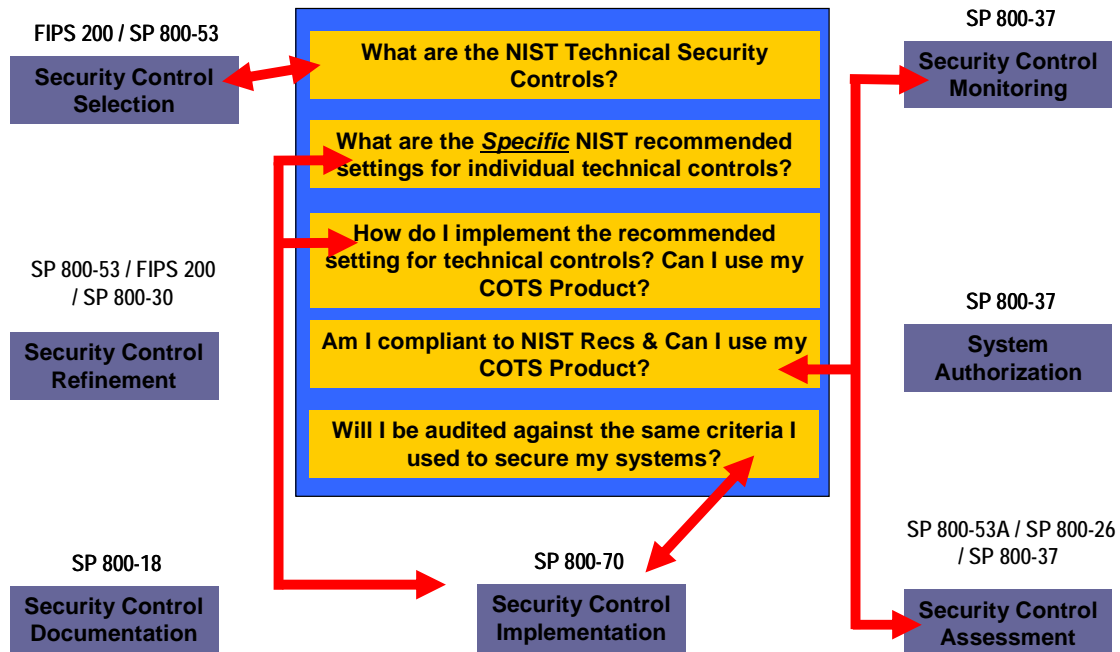
## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

agencies spent \$5.5 billion securing the government's total IT investment of approximately \$63 billion equating to approximately 9 percent of the total IT portfolio. Of course, not all of this was spent on FISMA compliance certification and accreditation, but many of the decisions pertaining to that \$5.5B in security infrastructure investment began with an assessment of overall security readiness within the context of any number of security methodologies such as NIACAP, DITSCAP(DIACAP), HIPAA, and ISO17799 (see earlier work done by this committee on the [Federal Information Security Regulatory Compliance Guide And Matrix](#)), many of these driven by the need to attain FISMA compliance.

It is beyond the scope of this paper to cover the complexities pertaining to the attainment and maintenance of FISMA compliance, however, a map of documentation reference material is provided in Figure 5: FISMA Documentation Scope in support of further investigation and research. This section lays the groundwork for the examples provided that describe how automation can be applied to improving the FISMA compliance process.

**Figure 5: FISMA Documentation Scope**



xiii

## FISMA Compliance - Operational Scenario – How It All Comes Together

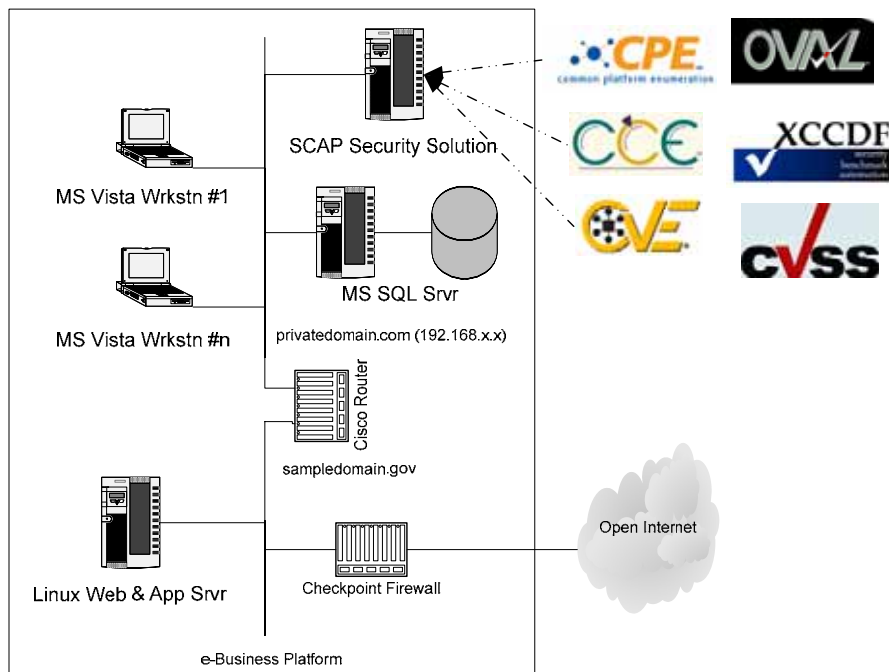
In order to better understand the power of the standards when combined into a comprehensive security solution based on COTS, GOTS, open-source and custom-developed software, a couple of simple operational scenarios are presented in this section.

For the purpose of these discussions, this hypothetical network (see Figure 6: Platform Under Test) is made up of the following components:

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

- Linux server with a combined web and application server;
- Windows server with SQLServer database;
- Several Windows Vista Workstations;
- Cisco Routers between the PrivateDomain.com – SampleDomain.gov;
- Checkpoint firewall between the SampleDomain.gov - Internet;
- Security solutions server running various SCAP-compliant tools, security data model and pipelined scripting of some XML data feeds used to integrate the tools located on the PrivateDomain.com;

Figure 6: Platform Under Test<sup>xiv</sup>



### Operation #1 – Unsuccessful Login Attempts - Federal Desktop Core Configuration

Many security vulnerabilities are the result of misconfigured systems and software. One initiative The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FDCC currently exists for Microsoft Windows Vista and XP operating system software. Currently, FDCC settings exist for Microsoft Windows XP Professional (Service Pack 2) and Microsoft Windows Vista Enterprise. The Windows Vista FDCC is

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

based on DoD customization of the Microsoft Security Guides for both Windows Vista and Internet Explorer 7.0. Microsoft's Vista Security Guide was produced through a collaborative effort with DISA, NSA, and NIST. The guide reflects the consensus recommended settings from DISA, NSA, and NIST for the Windows Vista platform. The Windows XP FDCC is based on Air Force customization of the Specialized Security-Limited Functionality (SSLF) recommendations in NIST SP 800-68 and DoD customization of the recommendations in Microsoft's Security Guide for Internet Explorer 7.0.

In this scenario, the security analyst uses a collection of tools to discover the devices connected to the subnetwork domain “sampledomain.gov” and “privatedomain.com” in preparation for FISMA Certification and Accreditation (C&A) as show in Figure 6: Platform Under Test.

The following tools descriptions are hypothetical examples and do not represent the functionality found in currently available tools. For a listing of [SCAP compliant technologies](#) and products, the following links are provided:

- [CVE Products](#)
- [OVAL Products](#)
- CCE Products – no product reference sites;
- CPE Products – no product reference sites;
- XCCDF Products – data repository site. no product reference sites;
- CVSS Products – no product reference sites.

NIST is in the process of establishing an SCAP Validation program via

Discovery Tool #1 uses the TCP/IP protocol and NMAP type of functionality to identify each of the devices connected to the network. Once this tool has identified and classified each device on the network, this information is passed to device specific tools capable of querying the configuration files of the workstations, servers, routers, and firewalls.

Configuration Management Tool #2 queries the configuration information from the Vista and XP desktop workstations connected to the network. This information is then analyzed and compared, on a workstation-by-workstation basis, with the applicable data defined in the SCAP-WinVista files listed below to determine if the unit under test (UUT) is properly configured:

**SCAP-WinVista-CPE.xml – product and platform identification information (see**

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

- Table 4: Excerpt from SCAP-WinVista-CPE.xml).
- SCAP-WinVista-OVAL-v90.xml – links human readable and reportable rule definitions with configuration parameters to support configuration testing and reporting.
- SCAP-WinVista-Patches.xml – links independent bug references (e.g. Bugtraq, CERT-VN) to CVE identifiers and product definitions.
- SCAP-WinVista-XCCDF.xml – defines what configuration and policy rules should invoked (tested) based on the risk level (800-53) for a given target.

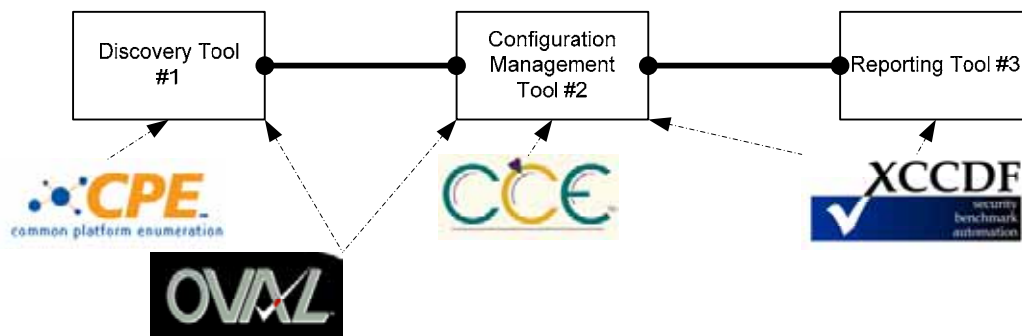
Reporting Tool #3 then takes the analysis generated by the Configuration Management Tool #2 and creates a report that can either be stored in a repository, emailed as an alert to a pager, or further pipelined to another tool that can schedule semi-automated or fully automated reconfigurations of the workstation experiencing a configuration issue.

**Figure 7: Integration Pipelining of Tools** shows how the input and outputs of these tools can be pipelined if these tools can consume files meeting the applicable SCAP standards and product information in the applicable SCAP format. A list of standards used in this example are shown in the figure.

One of the NIST rules highlighted in this example that is being tested is:

**AC-7 UNSUCCESSFUL LOGIN ATTEMPTS (from NIST SP800-53.pdf)** - Control: The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to [Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.

**Figure 7: Integration Pipelining of Tools – Configuration Compliance**



## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

As shown in Figure 7, the Discovery Tool #1 consumes information on the Federal Desktop Core Configuration (FDCC) compliant configuration identified in the OVAL and CPE files and uses this information to properly identify and classify one of the Vista Workstations on the network. This list of UUTs are then fed into the Configuration Management Tool #2 where further analysis is performed.

As shown in Figure 8, expected registry information is identified for comparison in the discovery tool to the queried registry data of the UUT. OVAL test #192 is to see if at least one instance of Windows Vista is installed in the UUT. The object and state reference values (2535 and 182) are used to identify this configuration to other data files within the defined namespace (XMLNS).

The CCE and OVAL files are then used by the Configuration Management Tool #2 to determine what policy rules, in the case of this example, should be tested to a “known good” configuration. Table 5 shows under definition 6010 that the “Audit Account Login” test should be performed. The link to CCE-315 provides a functional-regulatory cross-reference as shown in Table 6. By executing and verifying this single functional test for the Vista security policy for “Audit Account Login”, a number of regulatory standards can be verified.

As show in Table 7, for a “low” risk environment such as the PrivateDomain.com, the AC-7 Unsuccessful Login Attempts security policy should be enabled in order to comply with the 800-53 rule definition shown above. Once the Configuration Management Tool #2 has completed this test, the results are passed to the Reporting Tool #3 that uses the information contained in the applicable XCCDF and CVSS files to create a report.

# Improving FISMA Effectiveness and Efficiency Through the Security Content Automation Program (SCAP)

**Table 4: Excerpt from SCAP-WinVista-CPE.xml**

```
- <tests>
- <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
  id="oval:org.mitre.oval:tst:192" version="1" check="at least one" comment="Windows Vista is
  installed">
  <object object_ref="oval:org.mitre.oval:obj:2535" />
  <state state_ref="oval:org.mitre.oval:ste:182" />
</registry_test>
- <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
  id="oval:org.mitre.oval:tst:3653" version="2" check="at least one" comment="a version of
  Windows for the x64 architecture is installed">
  <object object_ref="oval:org.mitre.oval:obj:1576" />
  <state state_ref="oval:org.mitre.oval:ste:3180" />
</registry_test>
- <family_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
  id="oval:org.mitre.oval:tst:99" version="1" check="only one" comment="the installed operating
  system is part of the Microsoft Windows family">
  <object object_ref="oval:org.mitre.oval:obj:99" />
  <state state_ref="oval:org.mitre.oval:ste:99" />
</family_test>
</tests>
- <objects>
- <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
  id="oval:org.mitre.oval:obj:1576" version="1">
  <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:2535" version="1">
  <hive>HKEY_LOCAL_MACHINE</hive>
```

**Table 5: Excerpt of the Control Definition from SCAP-WinVista-OVAL-v90.xml**

```
</definition>
- <definition id="oval:gov.nist.1:def:6010" version="1" class="compliance">
- <metadata>
  <title>Audit Account Login</title>
  - <affected family="windows">
    <platform>Microsoft Windows Vista</platform>
  </affected>
  <reference source="CCE" ref_id="CCE-315" />
  <description>Audit Account Login</description>
  - <oval_repository>
    - <dates>
      - <submitted date="2007-04-05T13:57:10.000-05:00">
        <contributor organization="Secure Elements, Inc.">Sudhir Gandhe</contributor>
      </submitted>
      <status_change date="2007-04-05T13:57:10.000-05:00">DRAFT</status_change>
    </dates>
    <status>DRAFT</status>
  </oval_repository>
</metadata>
- <notes>
  <note>Secure Elements - Microsoft Windows Vista Benchmark</note>
</notes>
- <criteria operator="AND">
  <extend_definition definition_ref="oval:gov.nist.1:def:2" comment="Microsoft Windows Vista
  is installed" />
  <criteria test_ref="oval:gov.nist.1:tst:60101" negate="false" comment="Comments need to
  be added" />
</criteria>
</definition>
```

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

**Table 6: CCE File Cross-reference - windows\_cce\_4.0.xls**

CCE Id	CCE Definition	CCE Parameters	CCE Technical Mechanisms	DISA Stig for Windows 2003	NIST SCAP Windows Vista XCCDF (SCAP-WinVista-XCCDF.xml rev 2007-02-06)	NIST SCAP Windows Vista OVAL (SCAP-WinVista-OVAL.xml rev 2007-02-06)	NIST SCAP Office 2 (SCAP-Office2-OVAL-B)
CCE-315	The "audit account logon events" policy should be configured correctly.	(1) successful attempts audited gln (2) failed attempts audited gln	(1) defined by Local or Group Policy		audit-account-logon-events	oval.com.secure-elements.oval:def:6010	

**Table 7: Excerpt from the SCAP-WinVista-XCCDF.xml**

```
- <cpe:cpe-list>
- <cpe:cpe-item name="cpe://microsoft:windows:vista">
  <cpe:title>Microsoft Windows Vista (32-bit)</cpe:title>
  <cpe:check system="http://oval.mitre.org/XMLSchema/oval-definitions-5" href="SCAP-WinVista-CPE.xml">oval:org.mitre.oval:def:1282</cpe:check>
</cpe:cpe-item>
</cpe:cpe-list>
<platform idref="cpe://microsoft:windows:vista" />
<version>0.90</version>
<model system="urn:xccdf:scoring:default" />
<model system="urn:xccdf:scoring:flat" />
- <Profile id="Low-800-53" abstract="true">
  <title>800-53 Low</title>
  <description>This profile selects specific controls that are recommended by Special Publication 800-53 for information systems in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. Each control has an effect on other groups within this document as individual rule require certain controls to be selected.</description>
  <!-- ~~~~~ AC ~~~~~ -->
  <select idref="AC-1" selected="1" />
  <select idref="AC-2" selected="1" />
  <select idref="AC-3" selected="1" />
  <select idref="AC-4" selected="0" />
  <select idref="AC-5" selected="0" />
  <select idref="AC-6" selected="0" />
  <select idref="AC-7" selected="1" />
  <select idref="AC-8" selected="1" />
```

## Operation #2 – Continuous Monitoring – 24x7 Vulnerability Assessment

### CA-7 CONTINUOUS MONITORING

**Control:** The organization monitors the security controls in the information system on an ongoing basis.

**Supplemental Guidance:** Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization establishes the selection criteria for control monitoring and subsequently selects a subset of the security controls employed within the information system for purposes of continuous monitoring. NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls.

## Improving FISMA Effectiveness and Efficiency

### Through the Security Content Automation Program (SCAP)

Figure 8: Integration Pipelining of Tools – Constant Monitoring shows how application specific tools for security monitoring can be pipelined using the SCAP standards. In a manner similar to Operation #1, this operational environment provides constant monitoring of the UUTs to ensure 24x7 protection of the assets. The Discovery Tool #1 feeds configuration information to a tool that provides two discrete functions; intrusion detection and vulnerability management. The configuration information from the Discovery Tool #1 and the applicable CCE is consumed by the tool to establish certain operational profiles of the UUT and to identify when the TCP/IP traffic content deviates from these profiles. The vulnerability management function consumes CCE, XCCDF and CVE information to determine if the UUT is properly configured and has the appropriated patches in the software to prevent known attack vectors. Table 8: CVE Vulnerability from nvdCVE-modified.xml shows an excerpt of the data file describing a vulnerability along with a list of the effective software products and version.

Figure 8: Integration Pipelining of Tools – Constant Monitoring

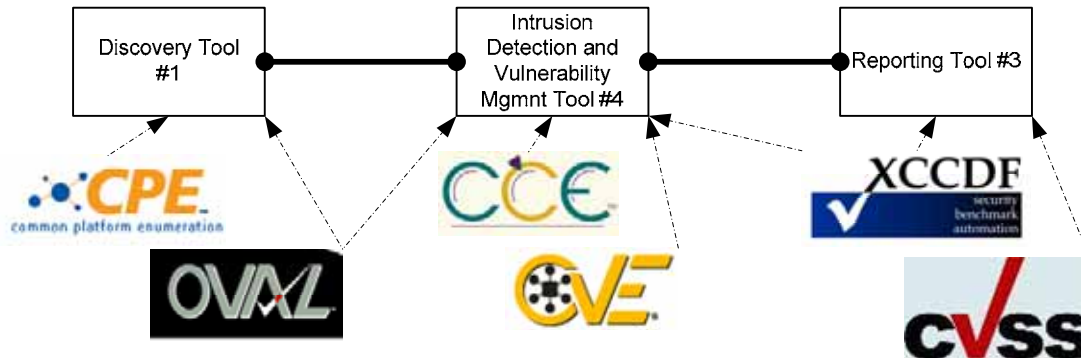


Table 8: CVE Vulnerability from nvdCVE-modified.xml

```
- <entry type="CVE" name="CVE-2007-2228" seq="2007-2228" published="2007-10-09" modified="2007-10-24" severity="High"
  CVSS_score="7.8" CVSS_vector="(AV:N/AC:L/Au:N/C:N/I:N/A:C)" CVSS_version="2.0" CVSS_base_score="7.8"
  CVSS_impact_subscore="6.9" CVSS_exploit_subscore="10.0">
- <desc>
  <descript source="cve">Unspecified vulnerability in the remote procedure call (RPC) component in Microsoft Windows XP
  SP2, XP Professional x64 Edition, Server 2003 SP1 and SP2, Server 2003 x64 Edition and x64 Edition SP2, and Vista
  and Vista x64 Edition allows remote attackers to cause a denial of service (RPCSS service stop and system restart)
  via a crafted RPC NTLMSSP authentication request. NOTE: this also affects Windows 2000 SP4, although the impact is
  an information leak.</descript>
  </desc>
- <loss_types>
  <avail />
  </loss_types>
- <range>
  <network />
  </range>
- <refs>
  <ref source="MS" url="http://www.microsoft.com/technet/security/Bulletin/MS07-058.msp">MS07-058</ref>
  </refs>
- <vuln_soft>
  - <prod name="windows" vendor="Microsoft">
    <vers num="2003 Server SP 1" />
    <vers num="2003 Server SP 2" />
    <vers num="2003 Server x64" />
    <vers num="2003 Server x64 SP2" />
    <vers num="vista" />
    <vers num="vista x64" />
    <vers num="xp sp2" />
    <vers num="2000 sp4" />
    <vers num="xp x64" edition="Professional" />
  </prod>
  </vuln_soft>
</entry>
```

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

**Recommendations:**

**Security Standards are Cost Effective**

The increasing complexity of security readiness have rendered the traditional manual methods for identifying vulnerable assets, assessing readiness, and creating the documentation to demonstrate compliance or to manage remediation clearly inadequate.

An enterprise-wide security compliance and management infrastructure that is integrated with the operations management platform (e.g. HP Openview, Tivoli Asset Management) is essential to achieving a high-level of security and operational readiness.

Standards are evolving that will reduce the costs, improve the efficiency and expand the effectiveness of regulatory requirements and industry best practices through:

- Automation
- Longitudinal consistency and repeatability
- Repurposing of data
- Pipelining of security test and monitoring systems
- Competitive sourcing

**Formal Certification Programs**

A formal security standards certification program is needed to ensure security practice (e.g. C&A) and tools conformance to the standards and to encourage the industry in the adoption and promulgation therein.

**Influence the Standards**

Agencies that become involved in the implementation of security standards and automation through the use of SCAP provide essential guidance and feedback to the continued development of such standards and the proper allocation and prioritization of IT talent and resources. Automation is complex; security is even more complex. A CIO committed to designing and building security compliant systems will build better IT platforms that are more reliable with higher availability and performance than those that are vulnerable and insecure.

**Upside and Downside of Business Process Automation**

Business process automation is expensive and complex, however, the return on investment of e-Business solutions (e.g. constituent self-service models), internal and external information processing projects has been repeatedly proven economically sound and practical.

However, the acquisition and maintenance of large data stores, particularly on websites, wireless devices, and mobile media formats such as laptops, PDAs and USB drives, has created new security challenges unknown just a few years ago. Now, it is as important to ensure the confidentiality, integrity and accessibility of these systems and the data protected by them through a comprehensive security management program as it is to automate in the first place. Agencies should not wait for the standards to fully mature before taking action. Security readiness and regulatory compliance are not achieved overnight. The mounting threats to national security and personal privacy are expanding minute-by-minute and the time for agency action is now.

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)

**Impact Statement:**

OMB FISMA E-Government Scorecard is an important way to measure and quantify the progress an agency has made with security readiness. There real-world threats of compromised national security and identify theft are increasing in both number and magnitude and are significantly more costly to remediate than prevention of the spying or theft.

Agencies that continue to implement security readiness and compliance programs through the traditional methods will experience ever increasing costs for labor, outsourced security expertise and indirect costs associated with insecure and vulnerable systems.

**Author(s) & Affiliations:**

The IAC Security & Privacy SIG would like to thank the following individuals for their efforts, expertise and contributions in bringing this product to fruition. This document is the product of contributors who volunteered countless hours of time and expertise in the development of this document:

**Federal Advisor**

- **Dennis Heretick, Chief Information Security Officer (CISO), Department of Justice**

**Principal Contributors**

- **Rob Roy Montgomery, President and Founder of Argosy Omnimedia, Inc. (Bethesda, MD)**
- **Scott Armstrong VP Marketing & Alliances of Secure Elements (Herndon, VA)**

**Contributors**

- **James Pettler, Sr. Research Analyst, Strategy, Governance, & Reporting, IDC-Government Insights**
- **Kenneth D. Suarez, President, Suarez Inc.**

Improving FISMA Effectiveness and Efficiency  
Through the Security Content Automation Program (SCAP)  
Bibliography

---

<sup>i</sup> Fiscal Year 2006 FISMA Report to Congress

<sup>ii</sup> Fiscal Year 2006 FISMA Report to Congress

<sup>iii</sup> Fiscal Year 2006 FISMA Report to Congress

<sup>iv</sup> The Security Content Automation Program (SCAP): Automating Compliance Checking, Vulnerability Management, and Security Measurement (Draft); Stephen D. Quinn, Peter Mell, Karen Kent (SCAP-NISTIR-7343.pdf)

<sup>v</sup> Fiscal Year 2006 FISMA Report to Congress

<sup>vi</sup> Fiscal Year 2006 FISMA Report to Congress

<sup>vii</sup> The Security Content Automation Program (SCAP): Automating Compliance Checking, Vulnerability Management, and Security Measurement (Draft); Stephen D. Quinn, Peter Mell, Karen Kent (SCAP-NISTIR-7343.pdf)

<sup>viii</sup> The Security Content Automation Program (SCAP): Automating Compliance Checking, Vulnerability Management, and Security Measurement (Draft); Stephen D. Quinn, Peter Mell, Karen Kent (SCAP-NISTIR-7343.pdf)

<sup>ix</sup> SPECIFICATION FOR THE EXTENSIBLE CONFIGURATION CHECKLIST DESCRIPTION FORMAT (XCCDF) VERSION 1.1.3, xccdf-spec-1.1.3-20070401-draft.pdf.

<sup>x</sup> 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>.

<sup>xi</sup> National Institute of Standards and Technology Interagency Report 7343 (Draft)

<sup>xii</sup> <http://www.first.org/cvss/cvss-guide.html#1.5>

<sup>xiii</sup> SCAP-webpp-10182006.ppt

<sup>xiv</sup> CVE is a registered trademark and the Making Security Measurable logo, CCE, CME, CWE, CPE, and OVAL are trademarks of The MITRE Corporation.