

**ABOUT**

**SRG, CCI, STIGs, Checklists, Tools, & Automation**

**Version 1 Release 1**

**Part of the:**

**SRG/STIG Applicability Guide and Tool**

**June 2014**

**Developed by DISA for the DoD**

This page is intentionally blank.

Table of Contents

Page

[1. Introduction 1](#_Toc385404133)

[1.1 Security Compliance Automation Protocol (SCAP) 1](#_Toc385404134)

[1.2 Extensible Configuration Checklist Description Format (XCCDF) 1](#_Toc385404135)

[1.3 Control Correlation Identifier (CCI) 2](#_Toc385404136)

[1.4 Security Requirements Guide (SRG) 2](#_Toc385404137)

[1.5 Security Technical Implementation Guides (STIGs) 3](#_Toc385404138)

[1.5.1 Classic STIG Format 3](#_Toc385404139)

[1.5.2 New STIG Format - XCCDF 3](#_Toc385404140)

[1.5.3 STIG Updates 4](#_Toc385404141)

[1.5.4 STIG Checklists 5](#_Toc385404142)

[1.5.5 STIG Checklist Updates 5](#_Toc385404143)

[1.6 Sunset / Archived Products 5](#_Toc385404144)

[1.7 Relationship between SRGs and STIGs 5](#_Toc385404145)

[1.8 Legacy STIGs and the Transition to the SRG model 6](#_Toc385404146)

[1.9 NIAP, Protection Profiles (PP), and DoD Annexes 6](#_Toc385404147)

[1.9.1 Relationship of DoD Annexes and PPs to STIGs 6](#_Toc385404148)

[1.10 SCAP Vulnerability Assessment and Policy Compliance Tools 7](#_Toc385404149)

[1.11 Open Vulnerability and Assessment Language (OVAL) 7](#_Toc385404150)

[1.12 Open Checklist Interactive Language (OCIL) 7](#_Toc385404151)

[1.13 Common Platform Enumeration (CPE) 8](#_Toc385404152)

[1.14 SCAP Benchmarks 8](#_Toc385404153)

[1.15 Benchmark Updates 9](#_Toc385404154)

[1.16 SCAP Validated Vulnerability and Compliance Scanning Tools 9](#_Toc385404155)

[1.16.1 Host Based Security System (HBSS) and McAfee Policy Auditor 9](#_Toc385404156)

[1.16.2 SCAP Compliance Checker (SCC) 10](#_Toc385404157)

[1.17 Unix and Database Scripts 10](#_Toc385404158)

This page is intentionally blank.

# Introduction

This document provides a discussion of, and definitions for, SRG, CCI, STIGs, Checklists, tools, compliance validation automation, and related topics. The intent is to orient the user of the SRG/STIG Applicability Guide and SRG/STIG Collection Tool to the technologies, standards, and terms used by DISA FSO as related to SRGs and STIGs.

## Security Compliance Automation Protocol (SCAP)

Security Compliance Automation Protocol (SCAP) is a National Institute of Standards (NIST) program. The technical specification for the SCAP is defined in NIST SP800-126 which states: SCAP “is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. SCAP is a multi-purpose framework of specifications that support automated configuration, vulnerability and patch 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.”

SCAP is part of NIST’s Federal Information Security Management Act (FISMA) implementation project. Under FISMA NIST is mandated to develop standards for the protection of the nation's critical information infrastructure.

The DoD SRGs and STIGs are migrating from various document formats to SCAP formats to foster compliance validation automation.

More information on NIST’s FISMA implementation project can be found at: <http://csrc.nist.gov/groups/SMA/fisma/index.html>

More information on SCAP can be found at <http://scap.nist.gov/index.html>:

## Extensible Configuration Checklist Description Format (XCCDF)

Extensible Configuration Checklist Description Format (XCCDF) is part of the SCAP.

From the NIST XCCDF web page <http://scap.nist.gov/specifications/xccdf/>:

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.

XCCDF documents are expressed in XML, and may be validated with an XML Schema-validating parser.

## Control Correlation Identifier (CCI)

**[Back = Alt🡨]**

The Control Correlation Identifier (CCI) provides a standard identifier and description for each of the singular, actionable statements that comprise an IA control or IA best practice. CCI bridges the gap between high-level policy expressions and low-level technical implementations. CCI allows a security requirement that is expressed in a high-level policy framework to be decomposed and explicitly associated with the low-level security setting(s) that must be assessed to determine compliance with the objectives of that specific security control. This ability to trace security requirements from their origin (e.g., regulations, IA frameworks) to their low-level implementation allows organizations to readily demonstrate compliance to multiple IA compliance frameworks. CCI also provides a means to objectively rollup and compare related compliance assessment results across disparate technologies.

The CCIs are based on the NIST SP 800-53 catalog of IA controls and enhancements, other DoD policy, and best practice, as referenced in the CCI. CCIs represent the smallest measurable facet of the IA control or policy from which it was derived. Each IA control and enhancement, DoD policy, and best practice generally begets multiple CCI. Currently, the CCI list contains the entire NIST SP 800-53 catalog of IA controls that have been decomposed into CCI. There are both policy CCI that are focused on the organization and technical CCI that are focused in the Information System (IS).

More information on CCI and the CCI list can be found at <http://iase.disa.mil/stigs/cci.html>.

## Security Requirements Guide (SRG)

A Security Requirements Guide (SRG) presents a compilation of DoD policy as a listing of CCI including the associated assessment and compliance criteria or methodology. As noted above, the CCIs are based on the NIST SP 800-53 catalog of IA controls and enhancements, other DoD policy, and best practice, as referenced in the CCI which represents the smallest measurable facet of the IA control or policy from which it was derived. The associated assessment methodology has been developed in coordination with the NIST SP 800-53A which provides general assessment methodology for the 800-53 IA controls.

Application of the individual IA controls and subsequently the subtended CCI will be dependent upon the pre-defined DoD baseline tailored to the risk categorization of the information system (IS) being addressed. Once the risk categorization is defined, the associated DoD baseline can be further tailored to the IS’ specific use case and environment by applying pre-defined overlays that can add or remove controls or change the default value of a control.

The IS risk categorization is derived as a combination of low (L), moderate (M), and high (H) impact (risk) levels for each category of Confidentiality, Integrity, and Availability. For example a public web server might have a risk categorization of low Confidentiality, medium Integrity, and medium Availability resulting in a designation of L,M,M. Note, there are 27 combinations. DoD has defined a baseline of applicable IA controls for each of the 27 combinations of L, M, and H for C, I, and A. The DoD baselines are published in the CNSSI 1253. The approved pre-defined overlays appear in appendices to the 1253 and are available from the CNSS website. Since the CNSSI 1253 applies to all National Security Systems (NSS) , whether classified or not, one very notable overlay is the Classified Information Overlay.

The determination of risk and application of the baselines as defined in the CNSS 1253 and its associated overlays is directed by the DoDI 8500.01 and DoDI 8510.01.

SRGs provide a generic set of IA requirements applicable to each of the coverage areas discussed below.

### SRG Coverage Areas

There are four core SRGs. These apply these CCI to: Organizational Policy; and, the three technology areas of: Networks; Operating Systems; and, Applications. The Policy SRG addresses Organizational Policy and incorporates NIST SP 800-53 IA controls and enhancements that reference the organization for compliance. The remaining three SRGs are technical in nature and incorporate those IA controls and enhancements that reference the Information System (IS) for compliance. These SRGs may also include some policy related controls and enhancements that the IS must support.

### Child SRGs

The four top level SRGs may spawn child SRGs that address various sub technologies under the main technology area. For example, the Application SRG has child SRGs covering Database, Application Server, and Web Server. The Network SRG also has child SRGs.

NOTE: This topic is intended as an introduction to the idea of child SRGs and will not provide a comprehensive list of child SRGs.

## Security Technical Implementation Guides (STIGs)

Currently Security Technical Implementation Guides (STIGs) come in two formats. These are discussed in the next two sub-sections.

### Classic STIG Format

The classic STIG format seen in older STIGs consists of a document that contains the background, scope, and authority for the STIG as well as other boilerplate information, a description of the technology being addressed, and the STIG requirements along with any associated discussion. Typically a checklist was published along with the STIG. While some STIGs exist in this format today, it is being deprecated in favor of a new format.

### New STIG Format - XCCDF

The new STIG format is aligned with the SCAP and its Extensible Configuration Checklist Description Format (XCCDF). As noted above, XCCDF is a format definition for .XML files containing checklist information. It contains much of the same information fields as the newer STIG Checklist format described in the next section.

The advantage of using XCCDF format is that the .xml files are ingestible by SCAP compliant compliance validation tools.

All new STIGs and major version updates are being published as a zipped package of files minimally consisting of the following:

* A STIG overview document containing the background, scope, and authority for the STIG as well as other boilerplate information, and a description of the technology being addressed.
* Optional VMS Asset registration instructions (sometimes part of the technology overview document).
* A read-me file that describes each file in the package
* The STIG in one or more zipped packages consisting of the following files:
  + One or more .XML files containing the set of XCCDF formatted STIG requirements and associated content. Each major XCCDF element includes the requirement, the vulnerability discussion, the assessment and compliance criteria or methodology, references, and other required fields.
  + A .XSL style sheet for displaying the STIG in a browser
  + A .jpg containing logos for use with the .XSL style sheet
* Other files deemed necessary or as provided by the STIG author.
* Some STIG packages also include OVAL (see tools below) benchmark related .XML files

### STIG Updates

Classically formatted STIGs were not updated except for major revisions and version changes. Required changes due to trouble tickets or the publication of new policy were addressed by updating the associated checklist during the formerly bi-monthly, now quarterly, maintenance update cycle. This was primarily due to the lengthy and involved STIG approval process which caused the STIG document to become out of sync with its checklist. As such, the checklist contained the most current information and requirements.

XCCDF formatted STIGs can now be updated more easily during the maintenance cycle. This means that issues with the content can be more easily corrected and the guidance will not get out of sync. Major changes in severity codes and added requirements (except for IAVM, INFOSEC level, and CYBERCOM order related items) will still need to process through the approval process.

The dates for the quarterly maintenance updates can be found here: <http://iase.disa.mil/stigs/fso_schedule.html>

### STIG Checklists

STIG Checklists were produced in the past in support of the associated STIG. Older checklists were merely a tabular means to check-off compliance with the STIG requirements. Newer checklists contain the assessment and compliance criteria or methodology associated with each requirement defined in its STIG. Some include a discussion of the vulnerability that drives the requirement and instructions for registering related assets in the DISA Vulnerability Management System (VMS).

### STIG Checklist Updates

No new checklists will be produced. STIG Checklists are being replaced by the new STIG format noted above. Existing checklists will only be updated if absolutely necessary.

## Sunset / Archived Products

Sunset products are older SRGs, STIGs, Checklists, or Tools (i.e., FSO Products) that may be relevant to the vendor products they address, but are no longer supported by FSO due to various reasons. The most common reason for this lack of FSO support is that the vendor product is outdated, superseded by a newer vendor product, or may be vendor non-support. Many such vendor products should not be in use thus there is no reason for FSO to maintain related products.

The lack of FSO support means that there is no active maintenance of the FSO product thus no updates of the product will be published. Lack of FSO maintenance means that any new vulnerability in the vendor’s product will not be captured for mitigation thus the FSO product either is, or will quickly become, out of date. Since FSO is no longer maintaining a given product, a SME responsible for, and knowledgeable about, the product may not be available thus customer support questions will most likely not be answerable.

Sunset products may be available from the IASE web site at <http://iase.disa.mil/stigs/sunset_products/index.html>, while other older products may be available via an email to FSO at [disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil](mailto:disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil) to request a copy from our archive.

## Relationship between SRGs and STIGs

Older or "legacy" Security Technical Implementation Guides (STIG) were based on Department of Defense (DoD) Instruction (DoDI) 8500.2 (Information Assurance (IA) Implementation) controls, various DoD policies, and best practice. Today, new STIGs are developed from Security Requirement Guides (SRG).

As discussed above, SRGs contain generic security requirements based on Control Correlation Identifiers (CCI) derived from Information Assurance (IA) controls in the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 IA control catalog.

STIGs based on SRGs provide vendor product specific configuration guidance and requirements that, when implemented, will cause the product to perform in a manner that meets each of the IA control and CCI requirements established in the parent SRG. Examples of new technology area product specific STIGs are the Apache 2.2 STIG, Red Hat 5 STIG, and SQL 2012 Database STIG. SRGs and new STIGs are published in Security Content Automation Protocol (SCAP) Extensible Configuration Checklist Description Format (XCCDF).

## Legacy STIGs and the Transition to the SRG model

Legacy STIGs were written toward specific technologies and toward areas of interest for the IA Certification and Accreditation community. These areas of interest range from entire Local Area Network or Campus Area Network (LAN/CAN) enclaves down to systems, individual devices, operating systems, and applications. These older STIGs are currently published in either SCAP XCCDF format or the older form of a written document and checklist. The large collection of legacy STIGs is being transitioned from document format to automatable SCAP XCCDF and will ultimately be replaced by SRGs and product specific SRG based STIGs. A mix of the three STIG formats (new SRG-based in SCAP XCCDF; legacy STIG in SCAP XCCDF; and legacy STIG in written document and checklist format) will exist for some time as this transition occurs.

## NIAP, Protection Profiles (PP), and DoD Annexes

The National Information Assurance Partnership (NIAP) – a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) – is responsible for U.S. implementation of the Common Criteria, including management of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) validation body. CCEVS manages a national program for developing protection profiles, evaluation methodologies, and policies that will ensure achievable, repeatable, and testable requirements. For more information regarding NIAP and the driving policies, see the [NIAP/Common Criteria Fact Sheet.](https://www.niap-ccevs.org/Documents_and_Guidance/cc_docs/NIAP_NCSC_factsheet.pdf) And the NIAP web site at <https://www.niap-ccevs.org/>

Common Criteria (CC) evaluations are performed against a technology specific Protection Profile (PP) which contains a set of Security Functional Requirements (SFRs) relavent to the technology area in which the test target operates. The test target must provide or comply with all SFRs in a PP. The result of a CC evaluation is “Pass All” or fail.

FSO coordinates with NIAP on the development of SRGs from which STIGs are developed. This coordination effort recognizes the existence of a PP for a given technology area such that a full DoD SRG will not be developed for the technology area. Instead, a DoD Annex for the PP will be developed that will contain any additional DoD requirements not contained in the PP. This will permit vendors having their products tested for CC to opt-in for additional testing against the DoD Annex. Once successful, the vendor can then develop a DoD STIG for their product.

### Relationship of DoD Annexes and PPs to STIGs

A DoD Annex to a PP provides the DoD specificity for the NIST SP 800-53 controls identified in the PP. As a result, the Annex, in conjunction with the PP, serves as a single specification, within the DoD, for security of the technology atea.

The publication of the Annex does not eliminate the DoD need for a product-specific Security Technical Implementation Guide (STIG); however, the results of the Common Criteria evaluation will be used to formulate a STIG. The benefit of this approach is that at the conclusion of a successful NIAP evaluation, a vendor's product will be certified as meeting the requisite NIST SP 800-53 controls and the information needed for a STIG will be available. The product may then be used within the DoD. STIGs will continue to be published in XCCDF format along with automation where applicable for assessment, as well as baseline configuration guidance for DoD.

## SCAP Vulnerability Assessment and Policy Compliance Tools

To address SCAP tools appropriately, a little background information needs to be provided in addition to the XCCDF content discussed above. This is the purpose of the next few sections.

## Open Vulnerability and Assessment Language (OVAL)

From Mitre.org <http://oval.mitre.org/index.html>:

OVAL is an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.

Tools and services that use OVAL for the three steps of system assessment — representing system information, expressing specific machine states, and reporting the results of an assessment — provide enterprises with accurate, consistent, and actionable information so they may improve their security. Use of OVAL also provides for reliable and reproducible information assurance metrics and enables interoperability and automation among security tools and services.

Additional information can be found at the mitre.org link above.

## Open Checklist Interactive Language (OCIL)

From the NIST CPE web page <http://scap.nist.gov/specifications/cpe/>:

The Open Checklist Interactive Language (OCIL) defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. Although the OCIL specification was developed for use with IT security checklists, the uses of OCIL are by no means confined to IT security. Other possible use cases include research surveys, academic course exams, and instructional walkthroughs.

In IT security, organizations work with security policies that detail the information that needs to be secured and the security requirements that must be met to ensure the information is protected accordingly. To verify compliance with security requirements, Federal agencies have already implemented security technologies that support the Security Content Automation Protocol (SCAP). OCIL is considered an emerging specification, so it is not currently included in SCAP. However, OCIL can still be used in conjunction with SCAP specifications such as XCCDF to help handle cases where lower-level checking languages such as OVAL are unable to automate a particular check. In short, OCIL provides a standardized approach to express and evaluate non-automated (i.e., manual) security checks.

Additional information can be found at the NIST.gov link above.

FSO is planning to provide OCIL based questionnaires to support required manual checks in the STIGs and general policy reviews in the automated SCAP benchmarks.

## Common Platform Enumeration (CPE)

From the NIST CPE web page <http://scap.nist.gov/specifications/cpe/>:

Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. CPE does not identify unique instantiations of products on systems, such as the installation of XYZ Visualizer Enterprise Suite 4.2.3 with serial number Q472B987P113. Rather, CPE identifies abstract classes of products, such as XYZ Visualizer Enterprise Suite 4.2.3, XYZ Visualizer Enterprise Suite (all versions), or XYZ Visualizer (all variations).

## SCAP Benchmarks

Under SCAP, a benchmark is a document that specifies settings and option selections that minimize the security risks associated with computer hardware or software.

A FSO published SCAP benchmark consists of security guidance written using the XCCDF language along with one or more validation languages such as OVAL and OCIL coupled with CPE. As such a FSO published benchmark is intended to contain the information needed to automate the evaluation of compliance with security guidance.

FSO will release new DoD SCAP benchmarks for various technologies as they are developed and approved. The latest available versions are available at: <http://iase.disa.mil/stigs/scap/index.html>.

NOTE: While a DoD STIG published in XCCDF format meets the basic definition of a benchmark, and while the XCCDF STIG names use benchmark naming standards, the use of the word “benchmark” in the name of a FSO published package indicates the ability for it to be used for automating the evaluation of compliance with security guidance.

## Benchmark Updates

FSO updates SCAP benchmark content as necessary to keep up with IAVMs and other policy changes. Updated benchmarks will be released during the quarterly STIG maintenance update cycle.

Scheduled FSO Release dates can be found at: <http://iase.disa.mil/stigs/fso_schedule.html>.

The latest available versions are available at: <http://iase.disa.mil/stigs/scap/index.html>.

## SCAP Validated Vulnerability and Compliance Scanning Tools

SCAP Vulnerability and Compliance Scanning Tools automate the process of vulnerability assessment and configuration policy compliance scanning of a particular IT asset or computing platform. SCAP tools ingest SCAP content consisting of various SCAP languages including XCCDF, OVAL, and OCIL, and enumerations such as CCE, CPE, and CVE to be used as the basis for assessing vulnerabilities and configuration policy compliance. The SCAP content can be in the form of an benchmark as discussed above.

NIST operates a SCAP validation program for SCAP Vulnerability and Compliance Scanning tools. This program validates that a vendor’s tool possesses the ability to use the features and functionality available through SCAP and its component standards.

SCAP validated tools will be used by DoD to assess the postures of DoD IT assets in the future. The transition has begun with the release of the XCCDF formatted STIGs and benchmarks.

NOTE: the various SCAP validated tools have varying capabilities. Not all are created equally and not all perform the same functions. Care must be exercised when selection a SCAP validated tool for use.

More information on SCAP content specifications can be found here: <http://scap.nist.gov/revision/1.2/>

More information on the tool validation program can be found here: <http://scap.nist.gov/validation/>

The list of SCAP validated tools can be found here:

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

### Host Based Security System (HBSS) and McAfee Policy Auditor

Policy Auditor is one of the McAfee point products that is part of DoD’s Host Based Security System (HBSS). Policy Auditor is an enterprise agent-based IT audit solution that leverages the SCAP to automate the processes required for internal and external IT audits.

Policy Auditor is one SCAP validated Vulnerability and Compliance Scanning Tool used by DoD.

### SCAP Compliance Checker (SCC)

The SCAP Compliance Checker (SCC) is a SCAP validated tool developed by the Navy’s Space and Naval Warfare (SPAWAR) Systems Center Atlantic. Its focus is currently limited to validating compliance with Federal Desktop Core Configuration (FDCC) standards or requirements as mandated by the Federal Office of Management and Budget (OMB).

## Unix and Database Scripts

In the past, DISA FSO produced vulnerability / compliance scanning tools in the form of scripts as follows:

* UNIX OS scripts for various varieties of UNIX and Linux
* Oracle Database scripts for Oracle running on UNIX/ Linux OSs
* Oracle Database scripts for Oracle running on Microsoft Windows OSs
* MS SQL Server Database scripts

These scripts automate the validation of as many of the associated UNIX and Database STIG requirements as were automatable in this manner.

These scripts have reached their end of life and are no longer being updated. As such, vulnerability detection for the OSs and products addressed by the scripts will be performed using SCAP compliant vulnerability / compliance scanning tools and OVAL benchmarks.