What are we changing?

To improve consistency, efficiency, accuracy, and automation of our STIGs, we are moving towards the adoption of the Security Content Automation Protocol (SCAP). The move to an eXtensible Configuration Checklist Description Format (XCCDF) formatted STIG provides the ability for the consumption of the STIGs by the various automated assessment tools, such as Host Based Security System (HBSS). This content not only can be consumed by these tools, but can also provide the detailed information on how to assess the system to determine compliance with the STIG requirement. This automation is only possible when Open Vulnerability Assessment Language (OVAL) code is available for the check being performed.

The STIGs will now be in extensible markup language (XML) format and include an XSL Transformations (XSLT) file to make the XML look more like a normal STIG. Some of the MS Word documents that were a part of the STIG will no longer be provided. There may be some MS Word documents included in the STIG zip file that contains introductory and background information that cannot be placed in the XML at this time. This would include such things as screen captures that help make the manual review process easier to understand.

STIG, STIG Checklist, or Checklist?

The term STIG, STIG Checklist, and Checklist have all been used to describe the DISA FSO generated security checklists. Starting in FY10, the term STIG will be used to describe the documents that provide the detailed security technical implementation guidance for the various technologies. Documents published prior to FY10 may still use the older terminology of STIG Checklist or Checklist but those will be changed to STIG as they are updated in future revisions of the document.

What is XCCDF?

The 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.

What is SCAP?

The SCAP is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality. Current SCAP protocols include: CVE, CCE, CPE, CVSS, OVAL and XCCDF.

http://scap.nist.gov/index.html

What is a Benchmark?

A benchmark is the version of the STIG content that contains the OVAL code that will allow tools to perform an automated assessment of the various checks. The benchmark does not contain all the checks that are necessary to meet the STIG requirements. The manual checks will still need to be addressed and those would be available in the Manual STIG.

What is a transformation?

An XML transformation language is a computer language designed specifically to transform an input XML document into an output XML document which satisfies some specific goal. XSLT is the best known XML transformation language. The transformation can be used to turn the XML document into something more appealing for viewing. For example, the STIG XML document can be transformed to look like a MS Word version of the STIG.

What is included?

The STIG will be packaged in a zip file that contains numerous files. There will be a readme file included in the zip file which is unique to that particular STIG. The readme.txt file will document the specific files for that technology.

Generally the following files will be included in the zip file (names may vary):

Readme.txt – Important info about the files for the particular technology.
STIG manual.xml – This is the STIG XML file that contains the manual check procedures.
STIG benchmark-xccdf.xml - This is the STIG XML file that contains the automated check procedures, and not the manual procedures. This file is only included for technologies that contain OVAL checks.

STIG.xsl – This is the transformation file that will allow the XML to be presented in a "human friendly" format.
Technology Overview.doc or .pdf – This file will contain the introductory and background information, as well as screen captures, network diagrams, and other important information that could not be stored in the XML file.
STIG-OVAL.xml – This file contains the detailed OVAL check code. This will only be provided if OVAL exists for the technology.
STIG-CPE-OVAL.xml - This is OVAL code that will provide information to the tool on how to check to see if the product being evaluated exists on the system.
STIG-CPE-DICTIONARY.xml – This is the file that contains the CPE information about the product.

How do I use it?

The STIG is still used the same way; it is just that the data is in a different format. To view the STIG, unzip the STIG and extract the files to a directory. Next, open the "STIG manual.xml" file in a browser window. The XSLT is already referenced in the XML file so the XML will open with the transformation applied and will appear as a normal document. From the browser the checklist can be printed or viewed on the screen. Depending on the technology, the printed report can become quite lengthy.

Can I print a report?

Yes you can still print a report. The STIG XML file will include a style sheet or transformation that will provide a view of the XML data in a more human readable format similar to what a STIG looks like today. This view can then be printed directly from your browser and would look similar to a printed STIG that came from a pdf or MS Word file. In addition, the XML file can be opened in MS Word. Depending on the technology, the printed report can become quite lengthy.

Is the old Word or PDF version of the checklist still available?

No. As technologies migrate to XCCDF, the MS Word versions of the STIG will cease to be maintained.

Acronym List

CCE - Common Configuration Enumeration
CPE - Common Platform Enumeration
CVE - Common Vulnerabilities and Exposures

CVSS - Common Vulnerability Scoring System
HBSS - Host Based Security System
OVAL - Open Vulnerability Assessment Language
SCAP - Security Content Automation Protocol
STIG - Security Technical Implementation Guide
XCCDF - eXtensible Configuration Checklist Description Format
XML - extensible markup language (XML)
XSLT - XSL Transformations