Defense Information Systems Agency

A Combat Support Agency

STIGs, SCAP and Data Metrics

Roger S. Greenwell, CISSP, CISA, CISM
Technical Director / Capabilities Implementation Division
DISA Field Security Operations

July 2010

DISA
A Combat Support Agency

Agenda

- STIG Overview
- Challenges faced in using STIGs and Checklists
- Security Content Automation Protocol (SCAP) Overview
- Reinventing STIGs using SCAP
- Metrics supported by SCAP

DISA
A Combat Support Agency

What is a STIG?

Security Technical Implementation Guide:

- A Compendium of DOD Policies, Security Regulations and Best Practices for Securing an IA or IA-Enabled Device (Operating System, Network, Application Software, etc.)
- A Guide for Information Security
- Mandated in DODD 8500.1, DODI 8500.2
- Endorsed by CJCSI 6510.01, AR 25-2, and AFI 33-202

Goals

- Intrusion Avoidance
- Intrusion Detection
- Response and Recovery
- Security Implementation Guidance

A Combat Support Agency

Policy References

- **DODD 8500.1**
  - Paragraph 4.18 All IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved **security configuration guidelines**.
  - Paragraph 5.1.8.4 DISA will develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.
- **DODI 8500.2**
  - E3.2.6 Security Configuration Specification. DISA and NSA support the Defense IA program through the development and dissemination of security implementations for the configuration of IA- and IA-enabled IT products. Examples of such specifications include Security Technical Implementation Guidelines (STIGS) and Security Recommendation Guides (SRG).
  - DCCS1/DCCS2 – A DOD reference document such as a **security technical implementation guide** or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled It products that require use of the product's IA capabilities. If a DOD reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a Departmental reference guide.
- **CJCSI 6510.01E, Enclosure C, 18a(7)**
  - Ensure STIGs or security recommendation guides are used as the baseline requirements being applied.
- **AR 25-2**
  - 4–5.f.(6) The minimum baseline configuration for ISs will be the published Security Technical Implementation Guide (STIG) requirements or the common criteria protection profiles for IA products, as available or supplemented and published by DOD and NETCOM/9th SC (A), with any changes documented.
- **AFI 33-202**
  - 3.6.3. Configuration Specifications. IA reference documents, such as National Institute of Standards and Technology (NIST) Special Publications, DoD Security Technical Implementation Guides (STIG), NSA Security Configuration Guides (SCG), AFI and/or AFMAN procedures, Air Force specialized publications (AFSSI, AF Technical Orders, etc.), AFCA guidance and other relevant publications represent a collection of resources for security configuration and implementation on the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. Ensure these reference documents are applied to establish and maintain a minimum baseline security configuration and posture.

A Combat Support Agency

Available STIGs

NETWORK/PERIMETER

Backbone Transport – V2R1, 9 Jul 07
Blackberry – V1R1, 23 Apr 10
Data Center Enclave – V4R4, 10 Feb 10
DATMS – V1R1, 30 Mar 04
DoD Internet-NIPRNet DMZ, - V1R2 26 Feb 10
DNS – V4R1, 17 Oct 07
DRSN – V1R1, 28 Mar 06
DSN – V2R3, 30 Apr 06
Enclave – V4R4, 18 Feb 10
Firewall STIG – V8R1 24 Mar 10
IDS-IPS STIG V8R1, 24 Mar 10
Infrastructure Router L3 Switch STIG V8R1, 24 Mar 10
L2 Switch STIG V8R1, 24 Mar 10
Other Devices STIG V8R1, 24 Mar 10
Network Policy STIG V8R1, 24 Mar 10
Perimeter Router L3 Switch STIG V8R1, 24 Mar 10
Secure Remote Computing, V2R1, 2 Oct 09
SPAN (Peripheral) – V1R1, 28 Jul 05
VOIP – V3R1, 23 Dec 09
Wireless – V6R1, 6 Aug 09

OPERATING SYSTEM

LPAR – V2R2, 4 Mar 05
MAC (APPLE)
Tandem – V2R2, 4 Mar 05
Unisys – V7R2, 28 Aug 06
UNIX – V5R1, 28 Mar 06
VM – V2R2, 4 Mar 05
Win 2003/XP/2000/Vista Addendum – V6R1, 21 May 07
Win NT (NSA)
Win 2000 – V6R1.16, 26 Feb 10
Win XP – V6R1.16, 26 Feb 10
Win2003 – V6R1.16, 26 Feb 10
Win Vista – V6R1.16, 26 Feb 10
Win Server 2008 (MS) – V6, R1.9, 26 Feb 10
Windows 7 – V1,R1 – 26 Apr 10
zOS – ACF2, V6R2, 25 Dec 09
zOS – RACF – V6R2, 25 Dec 09
zOS – TS – V6R2, 25 Dec 09

A Combat Support Agency

Available STIGs (cont.)

APPLICATIONS

AntiSpyware General – V4R1, 3 Dec 09
Application Services – V1R1, 17 Jan 06
Application Security & Development V3R1, 10 May 10
CITRIX XenApp, V1R1, 23 Jul 09
ESX Server - V1R1, 22 Apr 08
Database – V8R1, 19 Sep 07
Desktop Applications General – V4R1, 3 Dec 09
Directory Services – V1R1, 24 Aug 07
ERP – V1R1, 7 Dec 06
ESM – V1R1, 5 Jun 06
HBSS STIG – V2R5, 22 Feb 10
IM – V1R2, 15 Feb 08
InTFOT - V1R1, 2 Oct 09
ISA Server 2006 OWA STIG, V1R1 5 Feb 10
McAfee Antivirus – V4R1 – 3 Dec 09
Microsoft Exchange 2003 – V1R1, 6 Aug 09
MicrosoftIE6 – V4R1, 3 Dec 09
MicrosoftIE7 – V4R1, 3 Dec 09
MicrosoftIE8 – V1R1, 26 Apr 10
Microsoft Office 2003 – V4R1, 3 Dec 09
Microsoft Office 2007 – V4R1, 3 Dec 09
Mozilla Firefox – V4R1, 3 Dec 09
Symantec Antivirus – V4R1, 3 Dec 09
SunRay4 Thin Client – V1R1 – 26 Mar 09
VTC STIG – V1R1 – 08 Jan 08
Web Server – V6R1, 11 Dec 06

CROSS DOMAIN SOLUTIONS

JVAP Admin Procedures & Checklist
C2G Procedures & Checklist
Data Sync Procedures & Checklist
DII Procedures & Checklist
ISSE Procedures & Checklist
MLTC Procedures & Checklist
MLChat Procedures & Checklist
OWL Procedures & Checklist
RM Procedures & Checklist
SOWI Procedures & Checklist
TDX Procedures & Checklist
TGS Procedures & Checklist

USER

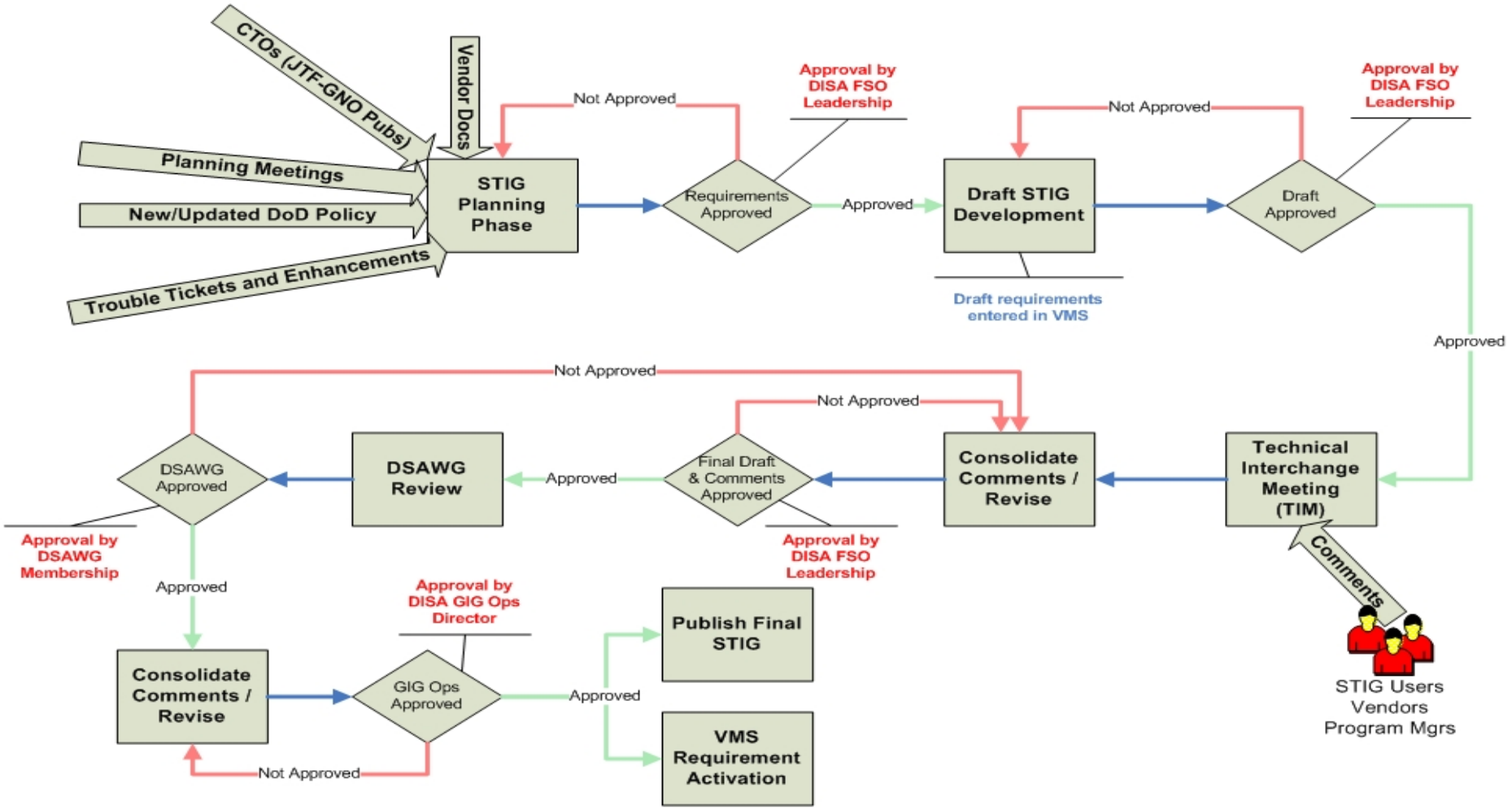
Access Control – V2R1, 17 Oct 07

STIGs are available at:
DKO: https://www.us.army.mil/suite/page/397960
IASE: http://iase.disa.mil/stigs/index.html

DISA
A Combat Support Agency

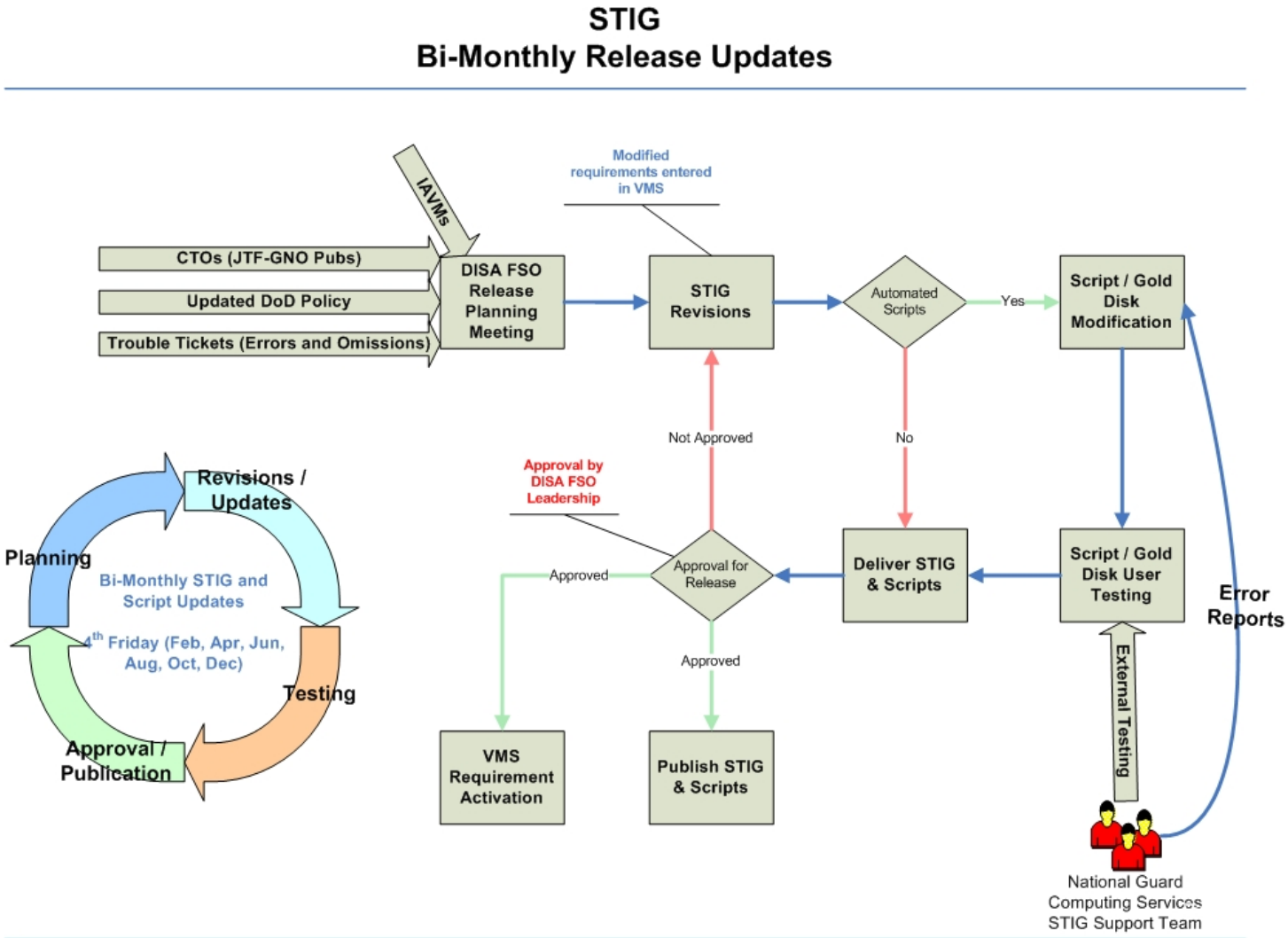
STIG Development Cycle

STIG
Version Updates / New Development



A Combat Support Agency

Bi-Monthly Release Lifecycle



DISA
A Combat Support Agency

Customer Challenges

- **Limited resources available to assess compliance with numerous requirements**
  - **Manual efforts**
  - **Impacts of different approaches for different technologies**
- **Understanding what documents apply (STIGs, checklists, varying technologies)**
- **Need for guidance in new technologies**
- **Support for new releases of technologies used**
- **Ability to extract information into other databases or products**

DISA
A Combat Support Agency

Maintenance Challenges

- High demand from the user community for new and updated security guidance
- Rapid pace of new technology
- Limited resources to develop guidance and tools to evaluate compliance
- Development and maintenance of varying tools/techniques for supporting compliance check
  - Gold Disk (Windows)
  - Security Readiness Review Scripts (Unix, some DB)

A Combat Support Agency

General Challenges

- **Secure Product Development**
  - No master list of all requirements for products
  - Vendors do not know, in detail, what requirements they have to meet
  - Not knowing “when they are done”
- **IA Compliance Reporting**
  - Determining compliance statistics
  - Inability to validate that all requirements are addressed in current checklists
  - Inconsistent reporting of findings and compliance status
- **Security Guide Development**
  - High Demand for New & Updated Security Guidance
  - Duplication of requirements
  - Interpretation of DoD IA Controls
  - Requirements not written in a measurable format
  - Inconsistency in documents from different sources

DISA
A Combat Support Agency

SCAP: Our Way Ahead

- **Security Content Automation Protocol (SCAP) is a collection of specifications**
  - **Specifications originally developed by the government which are now being adopted as the industry standard**
  - **Supports a standards based approach to develop and publish IA configuration guidance, assess assets, and report compliance**
- **Benefits of SCAP**
  - **Enables vendor community to develop standardized guidance once for use by all communities**
  - **Allow more commercial assessment tools to utilize DoD configuration guidance**
  - **Requires less time to develop and publish additional guidance**

More information on SCAP can be found at http://scap.nist.gov

DISA
A Combat Support Agency

SCAP Specifications

- CVE® - Common Vulnerabilities and Exposures
  - Common naming of emerging vulnerabilities
- CCE™ - Common Configuration Enumeration
  - Common naming of configuration (STIG) vulnerabilities
- CPE™ - Common Platform Enumeration
  - Language to describe Operating Systems/Platforms
- CVSS - Common Vulnerability Scoring System
  - Scoring System to describe severity of a vulnerability
- XCCDF - Extensible Configuration Checklist Description Format
  - XML definition of a checklist
- OVAL™ - Open Vulnerability and Assessment Language
  - Common language for assessing status of a vulnerability

- OCIL – Open Checklist Interactive Language (draft standard)
  - Common language to express questions to be presented to a user and interpret responses
- CCI – Control Correlation Identifiers (proposed by DISA)
  - Common identifier for policy based requirements
  - Currently not under SCAP umbrella

DISA
A Combat Support Agency

Moving Ahead for the Future

- **Migrating our tools and processes to take advantage of SCAP's benefit**
  - **The Policy Auditor Component of HBSS already supports assessing vulnerabilities using SCAP content**
- **Developing Security Requirements Guides (SRGs) that address overarching requirements for a technology (e.g. operating systems, network devices, applications, policy)**
  - **Promotes structure mapping of the STIGs to the new DoD Control Set**
- **Expanding work with operating system and software vendors to leverage content and standards**

A Combat Support Agency

Leveraging SCAP (XCCDF)

- **Publication of DoD content (STIGs) using the eXtensible Configuration Checklist Description Format (XCCDF)**
  - **Provides a standardized look for STIGs**
  - **Supports customers request to extract data for import into another database**
  - **XCCDF benchmarks can be used by SCAP capable tools to automate the assessment of vulnerabilities**
    - **Note that OVAL is required for true automation of a check**

A Combat Support Agency

Control Correlation Identifiers (CCIs)

- **A Control Correlation Identifier (CCI) is:**
  - A decomposition of an IA Control or an IA industry best practice into single, actionable statements
  - A foundational element of an IA policy or standard, written with a neutral position on an IA practice so as not to imply the specifics of the requirement
  - Not specific to a product or a Common Platform Enumeration (CPE).
- **The CCI List is:**
  - A collection of CCI Items, which express common IA practices or controls
- **The CCI data specification is:**
  - Proposed to work in conjunction with the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP)

A Combat Support Agency

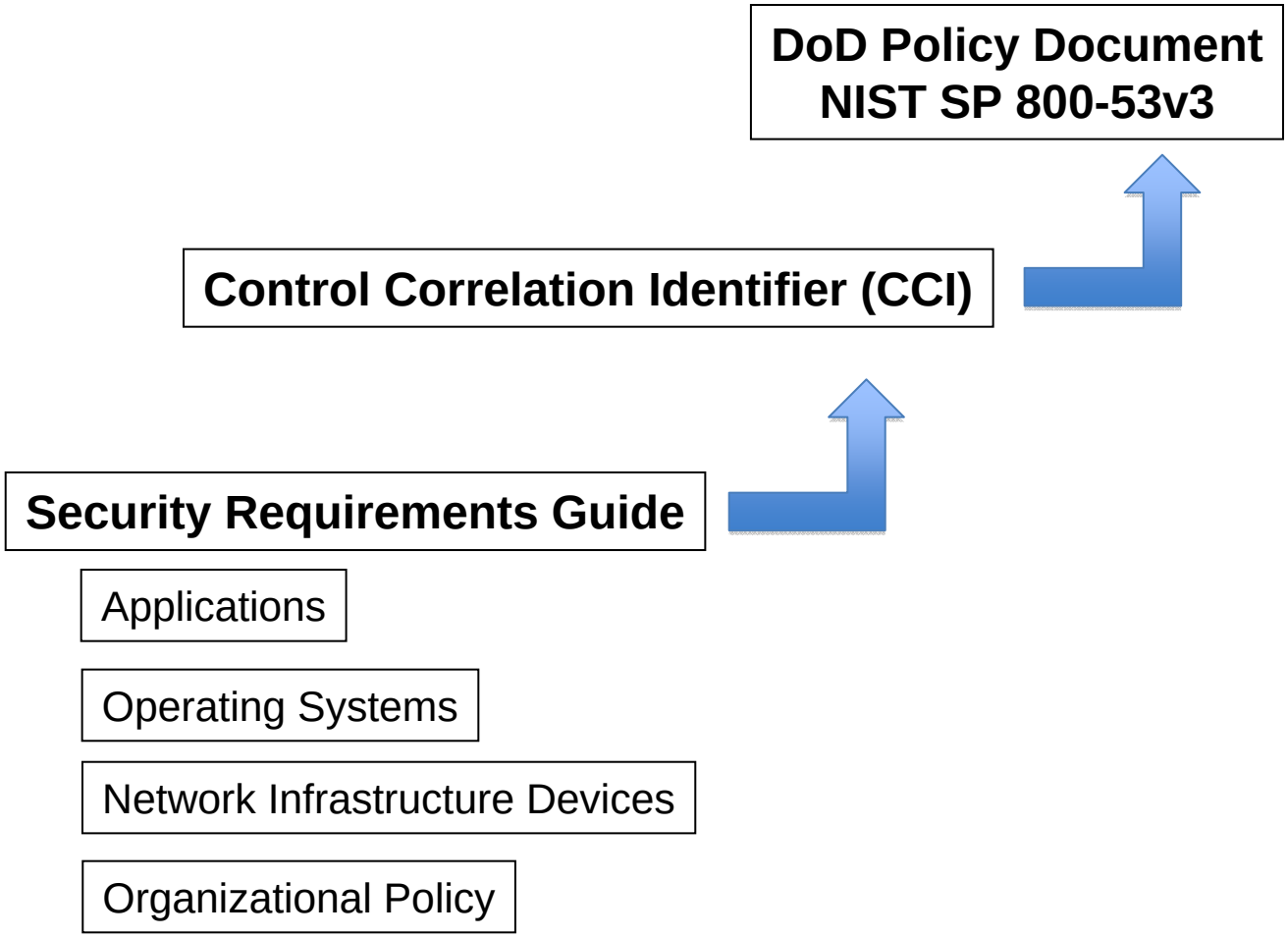
Security Requirements Guide (SRGs)

- **Similar to what a STIG is today**
  - Prose discussion of requirements
  - Planned SRGs include Operating System, Application, Network, Policy
  - Initial focus on Operating Systems to support UNIX development efforts
- **Will be expressed in XCCDF with the ability to produce a human readable version**
- **A method to convey additional technology specific details about the Common Control Identifiers (CCI) to product vendors**

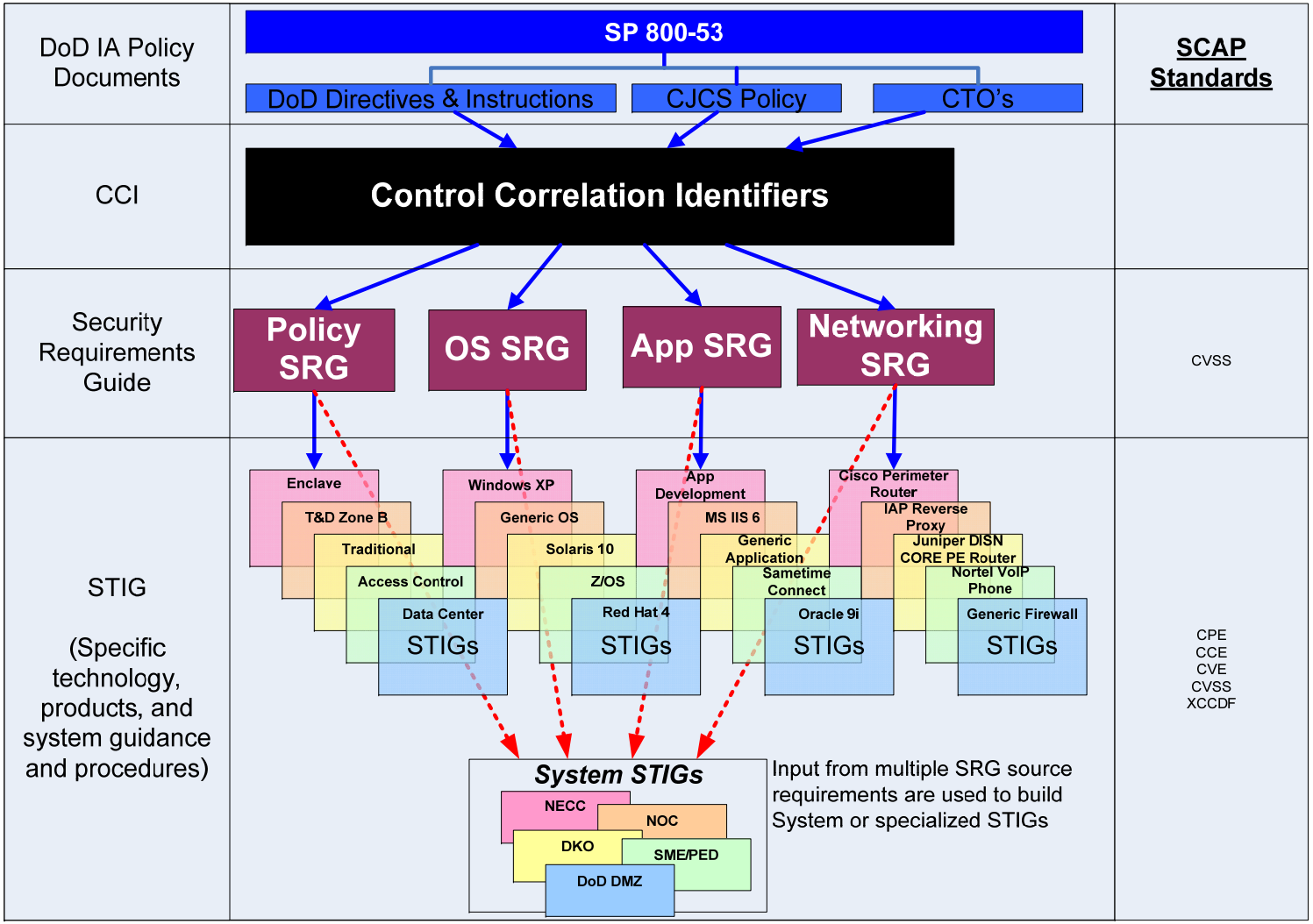
SRGs are not intended for use by Security Tool Vendors for assessments!

A Combat Support Agency

SRGs and CCIs



STIG Content – SCAP Enabled



A Combat Support Agency

SCAP Content Status

- **Windows STIG Content**
  - **Windows XP, Vista, 2003, 2008 published using XCCDF with OVAL**
    - **Many of the automatable configuration checks (e.g. STIG checks) have OVAL content available to support assessment of the vulnerability using SCAP compliant tools such as HBSS Policy Auditor**
- **UNIX STIG Content**
  - **UNIX Technical Interchange Meeting occurred in May 2010**
  - **Adopting approach of identifying SRG requirements to allow both in-house and vendor supported assessment of requirements**
- **Other STIG Content**
  - **20 different products supported with XCCDF Benchmarks**
    - **OVAL content not available**
- **IAVM Content**
  - **Working with the JFCC/NW-JTFGNO combined staff and NSA to determine best approaches for publishing IAVM content**

DISA
A Combat Support Agency

Metrics

- **Ongoing metrics analysis to identify trends/challenges observed throughout DoD**
  - **Goal to generate recommendations/approaches for material and/or non-material solutions or process enhancements**
- **Correlation and trending of vulnerability related information difficult given varying standards and repositories**
- **Leveraging industry standard approaches for identifying vulnerabilities is critical**
  - **Supported by existing SCAP standards**
- **Efforts underway to advance the reporting formats used as part of SCAP**

DISA
A Combat Support Agency

Summary

- **Adoption of a standards-based approach using SCAP addresses many of the key challenges that DoD faces today**
  - **Increased speed in publishing guidance to the IA community**
  - **Increased reliability of results based on industry standard checking mechanisms**
  - **Improved metrics and trending information relative to asset and vulnerability status**

DISA

A Combat Support Agency