DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Security Standards: Getting the Protections in Place

Christine McKinney
DISA Cyber Standards & Analysis Division
21 April 2016

Presentation Disclaimer

"The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to Unite States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments."

Agenda

- Authority
- Security Technical Implementation Guides
- Automation
- Impact

Authority

- **DoDI 8500. 01:**
  - **"2. DIRECTOR, DISA. Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in section 13 of this enclosure, the Director, DISA**
  - **b. Develops and maintains Control Correlation Identifiers (CCIs), Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), and mobile code."**

Cyber Standards and Analysis Division Mission

- Develop and maintain Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIGs)
- Guidance used in Command Cyber Readiness Inspection (CCRIs) and certification and accreditation (C&A) activities (compliance) as well as vendor product development
- Develop and disseminate operationally implementable secure configuration Guidance for use throughout the DoD
- Serve as the Information Systems Security Manager (ISSM) for the Risk Management Executive (RME) and Operations Center (OPC)
- Provide technical analysis and metrics support

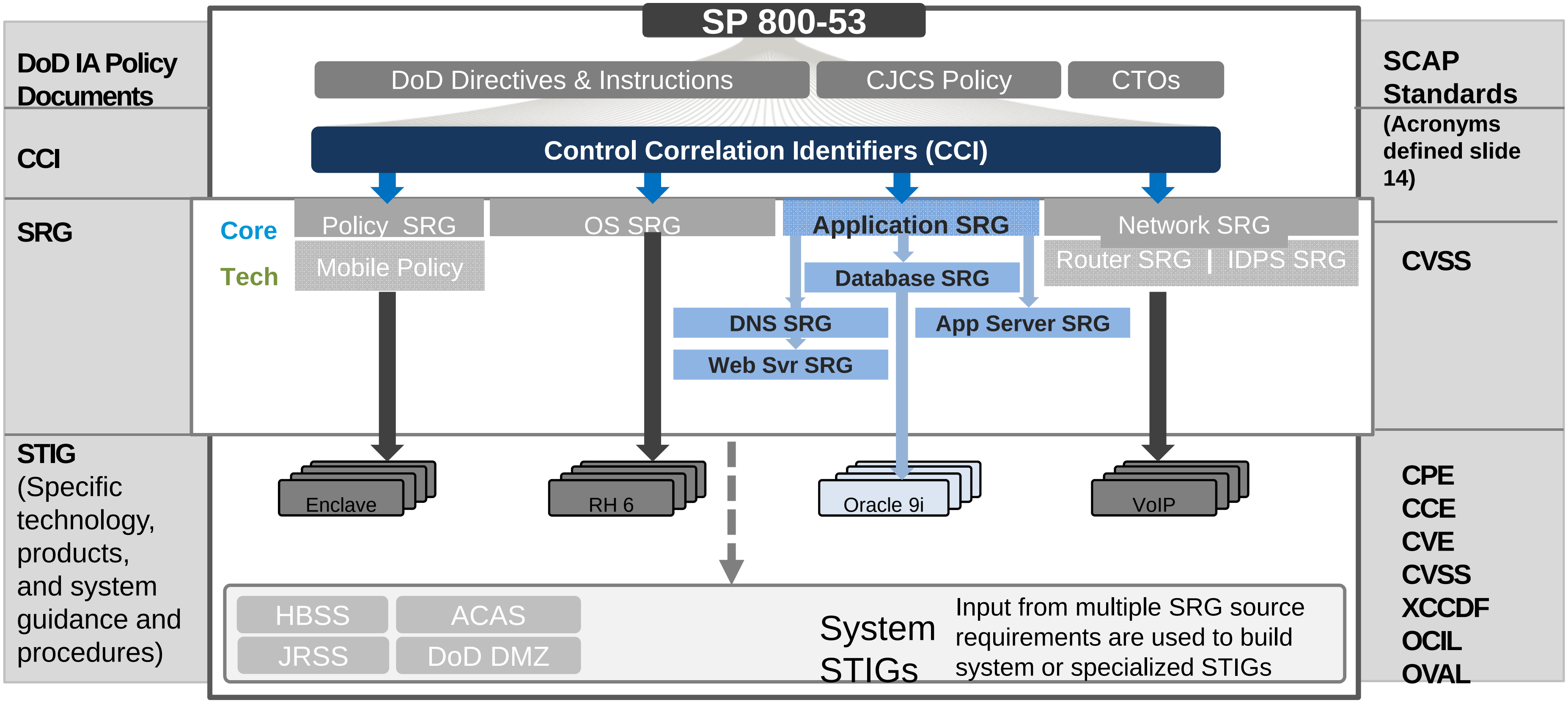
Priorities

- The STIGs support the DISA objectives
  - Joint Information Environment (JIE)
  - DoD Mobility Classified Capability (DMCC)
  - Cloud
  - Joint Regional Security Stacks (JRSS)
  - Software Defined Networking (SDN)

What is a STIG?

- Security Technical Implementation Guide:
  - An operationally implementable compendium of DoD IA controls, Security Regulations, and Best Practices for Securing an IA or IA-Enabled Device (Operating System, Network, Application Software, etc.)
  - Providing guidance for areas including mitigating insider threats, containing applications, preventing lateral movements, and securing information system credentials
- GOALS
  - Intrusion Avoidance
  - Intrusion Detection
  - Response and Recovery

STIG Model

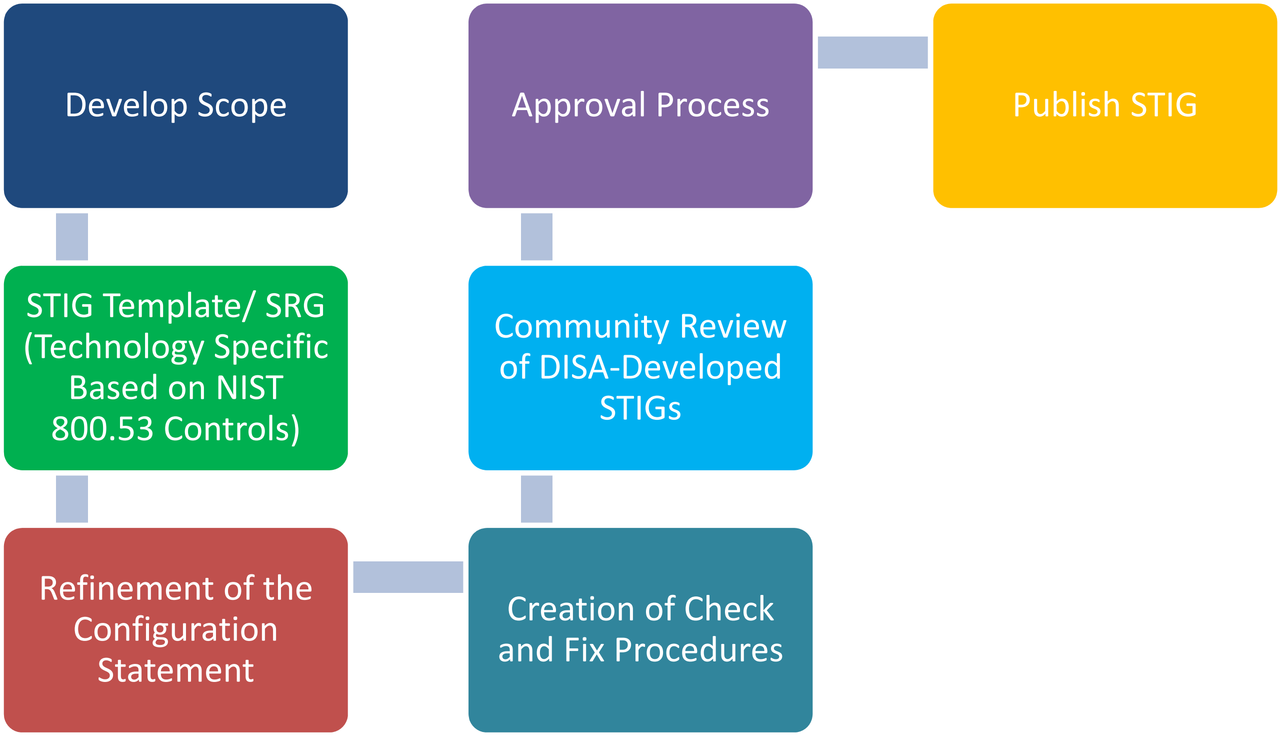

DoD IA Policy Documents
CCI
SRG
STIG
(Specific technology, products, and system guidance and procedures)
SP 800-53
DoD Directives & Instructions
CJCS Policy
CTOs
Control Correlation Identifiers (CCI)
Core
Tech
Policy SRG
Mobile Policy
OS SRG
Application SRG
Database SRG
DNS SRG
Web Svr SRG
App Server SRG
Network SRG
Router SRG | IDPS SRG
Enclave
RH 6
Oracle 9i
VoIP
HBSS
ACAS
JRSS
DoD DMZ
System STIGs
Input from multiple SRG source requirements are used to build system or specialized STIGs
SCAP Standards
(Acronyms defined slide 14)
CVSS
CPE
CCE
CVE
CVSS
XCCDF
OCIL
OVAL

Types of STIGs

- Policy and Architectural
  - Traditional/Physical Security
  - Facilities Security
  - Network Infrastructure Policy
- Technical:
  - DISA Cyber Standards team authors them with appropriated funding
  - Vendor Developed with assistance from the Cyber Standards team by submitting and intent form http://iase.disa.mil/stigs/Pages/vendor-process.aspx
  - Consensus partnering with military services and peer federal agencies

All NIST 800-53 Sourced

STIG Development Process



Develop Scope

STIG Template/ SRG (Technology Specific Based on NIST 800.53 Controls)

Refinement of the Configuration Statement

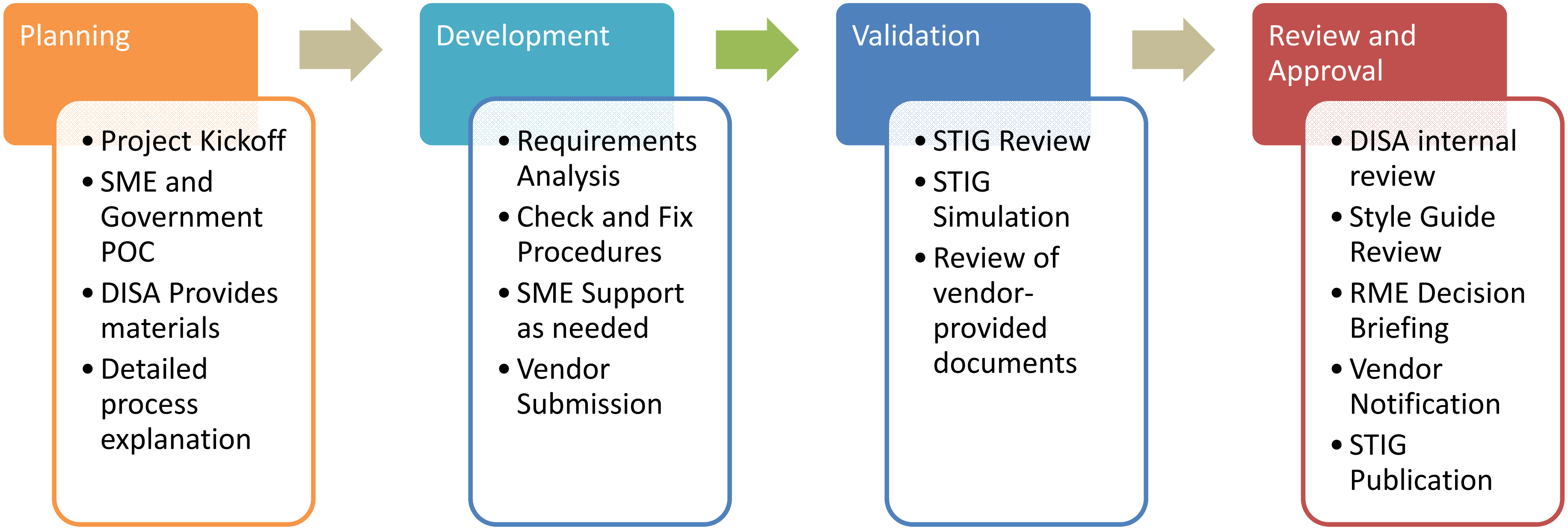
Creation of Check and Fix Procedures

Community Review of DISA-Developed STIGs

Approval Process

Publish STIG

Vendor STIG Process



Planning

- Project Kickoff
- SME and Government POC
- DISA Provides materials
- Detailed process explanation

Development

- Requirements Analysis
- Check and Fix Procedures
- SME Support as needed
- Vendor Submission

Validation

- STIG Review
- STIG Simulation
- Review of vendor-provided documents

Review and Approval

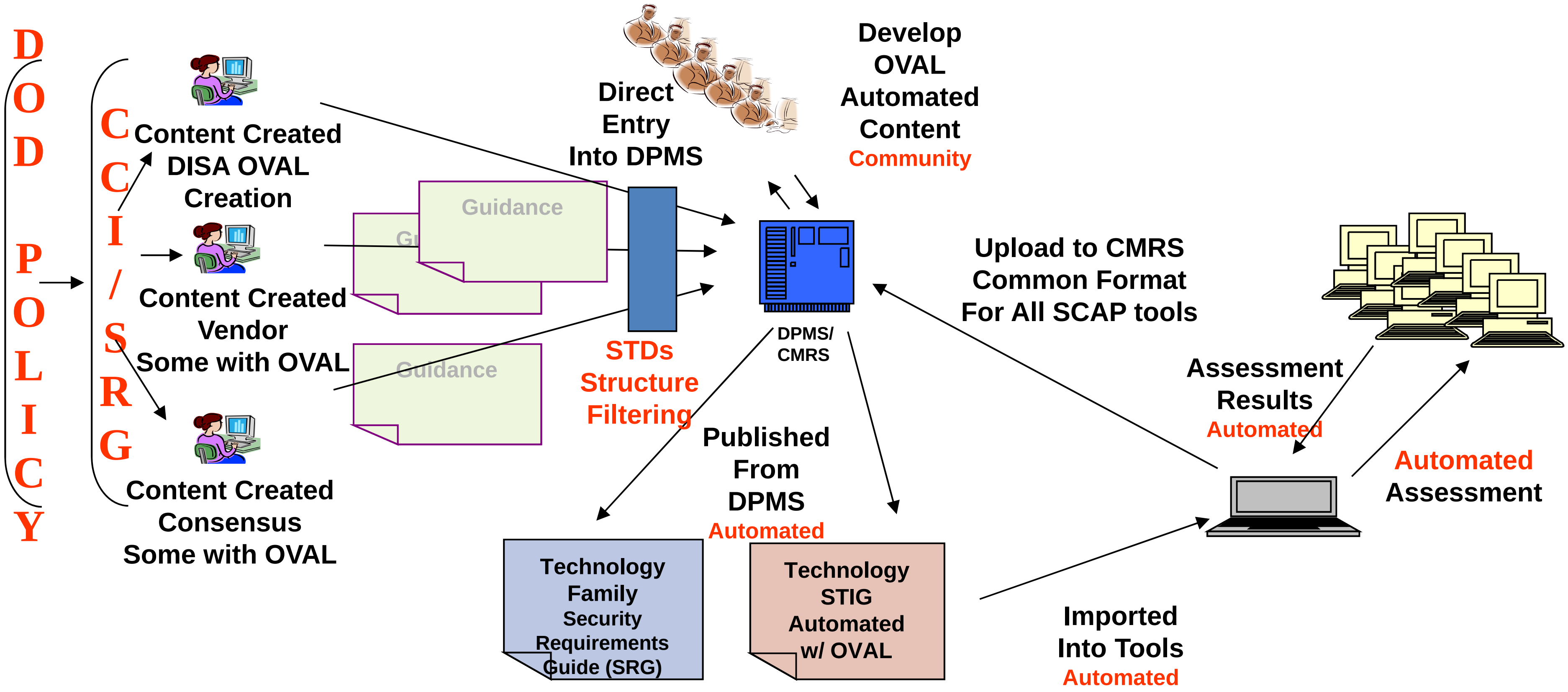
- DISA internal review
- Style Guide Review
- RME Decision Briefing
- Vendor Notification
- STIG Publication

DISA

Consensus Process

- **Participants include:**
  - **DoD Services and Agencies**
  - **Federal Agencies**
  - **NSA**
  - **Vendors**

Cyber Standards and Analysis Division View of STIG Automation



DOD POLICY

CCI / SRG

Content Created DISA OVAL Creation

Content Created Vendor Some with OVAL

Content Created Consensus Some with OVAL

Guidance

Guidance

Guidance

Direct Entry Into DPMS

STDs Structure Filtering

Develop OVAL Automated Content Community

DPMS/ CMRS

Upload to CMRS Common Format For All SCAP tools

Published From DPMS Automated

Technology Family Security Requirements Guide (SRG)

Technology STIG Automated w/ OVAL

Assessment Results Automated

Automated Assessment

Imported Into Tools Automated

Automation

- **Security Content Automation Protocol (SCAP)**
  - **A standards-based approach to develop IA configuration guidance, publish IA guidance, assess assets, and report compliance**

- **Benefits**
  - **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**

Core Security Content Automation Protocol Components

- Automated standardized machine-consumable security content leveraging several xml protocols presented below
- CPE – Common Platform Enumeration
- CVE – Common Vulnerably Enumeration
- CCE – Common Configuration Enumeration
- XCCDF – eXtensible Checklist Configuration Description Format
- OVAL – Open Vulnerability Assessment Language
- CVSS – Common Vulnerability Scoring System
- OCIL – Open Checklist Interactive Language

Why SCAP?

- Many Reasons
  - Open Standards
  - Supports many tools
  - Abstracts the “How”
  - Reduces development time
  - Repeatable
  - Non-Proprietary
  - Standard Identifiers
  - Lowers duplication efforts
  - Enterprise capability

DISA Produced Benchmarks

- HP-UX 11.31 / 11iv3
- IBM AIX 6.1
- Microsoft .NET Framework 4
- Microsoft Internet Explorer
- Microsoft Office
- Microsoft Windows
- Red Hat Enterprise
- Solaris

Where do I get the content?

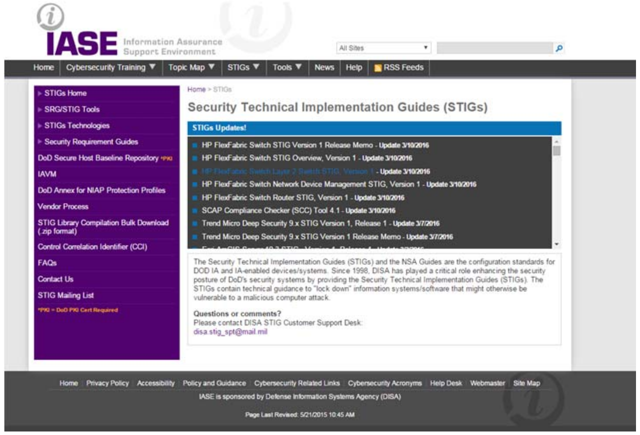
- There are over 16,000 registered users
- Over 920,000 hits per month
- Support for users questions in excess of 3000 each year

http://iase.disa.mil/stigs/index.html

Go Here

What is there?

- Access to over 300 security guides
- Mapped to both Federal NIST 800-53 and DoD CNSS-1253 IA control sets
- Manual and Automated (SCAP) Content
- STIG Viewer
- STIG Applicability Tool
- Windows 10 Secure Host Baseline Download


IASE Information Assurance Support Environment
All Sites
Home
Cybersecurity Training
Topic Map
STIGs
Tools
News
Help
RSS Feeds
STIGs Home
SRG/STIG Tools
STIGs Technologies
Security Requirement Guides
DoD Secure Host Baseline Repository *PKI
IAVM
DoD Annex for NIAP Protection Profiles
Vendor Process
STIG Library Compilation Bulk Download (.zip format)
Control Correlation Identifier (CCI)
FAQs
Contact Us
STIG Mailing List
*PKI = DoD PKI Cert Required
Home > STIGs

Security Technical Implementation Guides (STIGs)

STIGs Updates!

- HP FlexFabric Switch STIG Version 1 Release Memo - **Update 3/10/2016**
- HP FlexFabric Switch STIG Overview, Version 1 - **Update 3/10/2016**
- HP FlexFabric Switch Layer 2 Switch STIG, Version 1 - **Update 3/10/2016**
- HP FlexFabric Switch Network Device Management STIG, Version 1 - **Update 3/10/2016**
- HP FlexFabric Switch Router STIG, Version 1 - **Update 3/10/2016**
- SCAP Compliance Checker (SCC) Tool 4.1 - **Update 3/10/2016**
- Trend Micro Deep Security 9.x STIG Version 1, Release 1 - **Update 3/7/2016**
- Trend Micro Deep Security 9.x STIG Version 1 Release Memo - **Update 3/7/2016**

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

Questions or comments?
Please contact DISA STIG Customer Support Desk:
disa.stig_spt@mail.mil

IASE is sponsored by Defense Information Systems Agency (DISA)

Page Last Revised: 5/21/2015 10:45 AM

STIG Impacts

- **Internal analysis has shown over 96% of cyber incidents could have been prevented if STIGS were applied**
- **Rapid response to real-time cyber attacks**
- **Industry and government can benefit from security standards**

STIG Support Help Desk disa.stig_spt@mail.mil

Questions