Security Standards: Getting the Protections in Place

Christine McKinney
DISA Cyber Standards & Analysis Division
21 April 2016
"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
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 (CCRI) 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

Policy SRG
OS SRG
Application SRG
Network SRG

Core Tech

Mobile Policy

File SRG
Database SRG
App Server SRG

Enclave
RH 6
Oracle 9i
VoIP

STIG (Specific technology, products, and system guidance and procedures)

HBSS
ACAS
JRSS
DoD DMZ

Input from multiple SRG source requirements are used to build system or specialized STIGs

UNCLASSIFIED
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](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

1. Develop Scope
   - STIG Template/ SRG (Technology Specific Based on NIST 800.53 Controls)
2. Refinement of the Configuration Statement
3. Approval Process
   - Community Review of DISA-Developed STIGs
4. Creation of Check and Fix Procedures
5. 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
Consensus Process

**Participants include:**

- DoD Services and Agencies
- Federal Agencies
- NSA
- Vendors
Cyber Standards and Analysis Division View of STIG Automation

1. DOD Policy
   - CCI/SRG
   - DOD

2. Content Created
   - DISA OVAL Creation
   - Vendor
   - Some with OVAL
   - Consensus
   - Some with OVAL

3. Direct Entry Into DPMS
   - Guidance
   - Standards Structure Filtering

4. Upload to CMRS Common Format For All SCAP tools
   - Automated
   - Automated Assessment

5. Published From DPMS Automated
   - Technology Family Security Requirements Guide (SRG)

6. Technology STIG Automated w/ OVAL

7. Content Created by DISA OVAL

8. Content Created by Vendor

9. Some with OVAL

10. Consensus

11. Some with OVAL

12. Automated

13. Automated

14. Automated

15. Automated

16. Automated

17. Automated

18. Automated

19. Automated

20. Automated

21. Automated

22. Automated

23. Automated

24. Automated

25. Automated

26. Automated

27. Automated

28. Automated

29. Automated

30. Automated

31. Automated

32. Automated

33. Automated

34. Automated

35. Automated

36. Automated

37. Automated

38. Automated

39. Automated

40. Automated

41. Automated

42. Automated

43. Automated

44. Automated

45. Automated

46. Automated

47. Automated

48. Automated

49. Automated

50. Automated

51. Automated

52. Automated

53. Automated

54. Automated

55. Automated

56. Automated

57. Automated

58. Automated

59. Automated

60. Automated

61. Automated

62. Automated

63. Automated

64. Automated

65. Automated

66. Automated

67. Automated

68. Automated

69. Automated

70. Automated

71. Automated

72. Automated

73. Automated

74. Automated

75. Automated

76. Automated

77. Automated

78. Automated

79. Automated

80. Automated

81. Automated

82. Automated

83. Automated

84. Automated

85. Automated
• **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
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


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
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