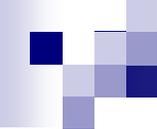


# Overview of NIST's SCAP Publications

Karen Scarfone, NIST



# Outline

- Publication Categories
- Pre-SCAP Publications
- Current SCAP Publications
- Future Publication Topics
- Special Publication 800-70 Revision 1

# NIST Publication Types

- Federal Information Processing Standard (FIPS)
  - Mandatory
- Special Publication (SP)
  - Recommendations
- Interagency Report (IR)
  - Informational (no recommendations)

**All planned SCAP publications are SPs and IRs**

# SCAP Publication Purposes

- SCAP Fundamentals
  - Define SCAP
  - Describe its use
  - Explain SCAP procedures, infrastructure, etc.
- SCAP Component Specifications
  - Define specifications that are not defined elsewhere
  - Explain how SCAP components can be tailored for Federal agency use
- SCAP Content Supplements
  - Explains the rationale behind configuration settings
  - Recommends additional non-automated controls

# Pre-SCAP Publications

## ■ Fundamentals

- SP 800-70, *Security Configuration Checklists Program for IT Products*
- SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*

## ■ Component Specifications

- IR 7275, *Specification for the Extensible Configuration Checklist Description Format (XCCDF)*

## ■ Content Supplements

- SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals*

# Fundamentals: Current

- IR 7511, *SCAP Validation Program Test Requirements (Draft)*
  - For accredited laboratories and IT product vendors
  - Defines the components (and versions, where applicable) that comprise SCAP version 1
  - Defines requirements that products must meet
  - Late comments still being accepted
- SP 800-70 Revision 1, *National Checklist Program for IT Products (Draft)*
  - For checklist users and developers

# Fundamentals: Future

- SP 800-117, *Managers' Guide to Adopting and Using SCAP (working title)*
  - Makes recommendations for using SCAP and for incorporating SCAP into IT products and services
- SP on technical aspects of using SCAP
  - Counterpart to SP 800-117
  - Customizing content
- Update to SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*

# Component Specs: Current

- IR 7275 Revision 3, *Specification for XCCDF Version 1.1.4*
  - Defines the current version of XCCDF
- IR 7435, *CVSS and Its Applicability to Federal Agency Systems*
  - Defines CVSS version 2.0
  - Explains how FIPS 199 impact levels can be used to tailor CVSS scores

# Component Specs: Future

- IR on CVSS scoring for NVD
  - Supplement to IR 7435
  - Documents how NVD analysts perform CVSS scoring based on the CVSS v2 specification
- IR 7502, *The Common Configuration Scoring System (CCSS) (Draft)*
  - Based on CVSS, customized for security configuration vulnerabilities
  - Defines first part of CCSS version 1.0
- Evolving Standards workshop on Thursday
  - CCSS, Common Configuration Identifier (CCI), Common Reporting Format (CRF), Open Vulnerability and Remediation Language (OVR)

# Content Supplements

- SP 800-68 Revision 1, *Guide to Securing Microsoft Windows XP Systems for IT Professionals (Draft)*
  - Includes references to FDCC baseline
  - Briefly discusses Service Pack 3
  - Public comment period closed
- New SP on securing Windows Vista systems
  - Describes some new security features
  - References FDCC and Microsoft baselines
  - To be released later this year

# Publication Summary

Fundamentals	<ul style="list-style-type: none"><li>■ SCAP Validation test requirements</li><li>■ National Checklist Program</li><li>■ Managers' guide to SCAP</li><li>■ Technical guide to SCAP</li><li>■ Patch management guide update</li></ul>
Component Specifications	<ul style="list-style-type: none"><li>■ XCCDF</li><li>■ CVSS</li><li>■ CCSS</li><li>■ CVSS analysis for NVD</li></ul>
Content Supplements	<ul style="list-style-type: none"><li>■ XP Pro</li><li>■ Vista</li></ul>

# National Checklist Program (NCP)

- Security checklist repository with metadata on contributed checklists
  - Prose documentation, configuration files, SCAP data streams, etc.
- Search engine for checklist selection
  - Keyword search, view by product category, view by vendor, etc.
- Formal process for submitting checklists to the repository

<http://checklists.nist.gov/>

# SP 800-70 Revision 1

- Describes the NCP and defines its operational procedures
- Defines all the checklist metadata fields
- Explains how end users can use the NCP
- Explains how checklist developers can participate
  - Provides a participation agreement form
- Defines operational environments for checklists
  - Managed, Standalone, Custom (FDCC, Legacy, and Specialized Security-Limited Functionality [SSLF])
- Proposes tiers to help checklist users

# Proposed Checklist Tiers

<b>Tier</b>	<b>Machine Readable</b>	<b>Automated Format</b>	<b>References to Security Compliance Framework</b>
<b>1</b>	No	N/A	Optional
<b>2</b>	Yes	Non-standard (proprietary, product-specific, etc.)	Optional
<b>3</b>	Yes	One or more SCAP components, not full SCAP data stream	Required; vetted with an entity authoritative for the framework
<b>4</b>	Yes	Complete SCAP data stream	Required; vetted with an entity authoritative

# SP 800-70 Revision 1 Feedback

- Posted for public comment
  - <http://csrc.nist.gov/publications/PubsDrafts.html>
- Deadline is Friday, October 31<sup>st</sup>
- Send comments to [800-70comments@nist.gov](mailto:800-70comments@nist.gov)

# Publication Links

- Special Publications

<http://csrc.nist.gov/publications/PubsSPs.html>

- Interagency Reports

<http://csrc.nist.gov/publications/PubsNISTIRs.html>

- Draft Publications

<http://csrc.nist.gov/publications/PubsDrafts.html>

## Questions?

[karen.scarfone@nist.gov](mailto:karen.scarfone@nist.gov)