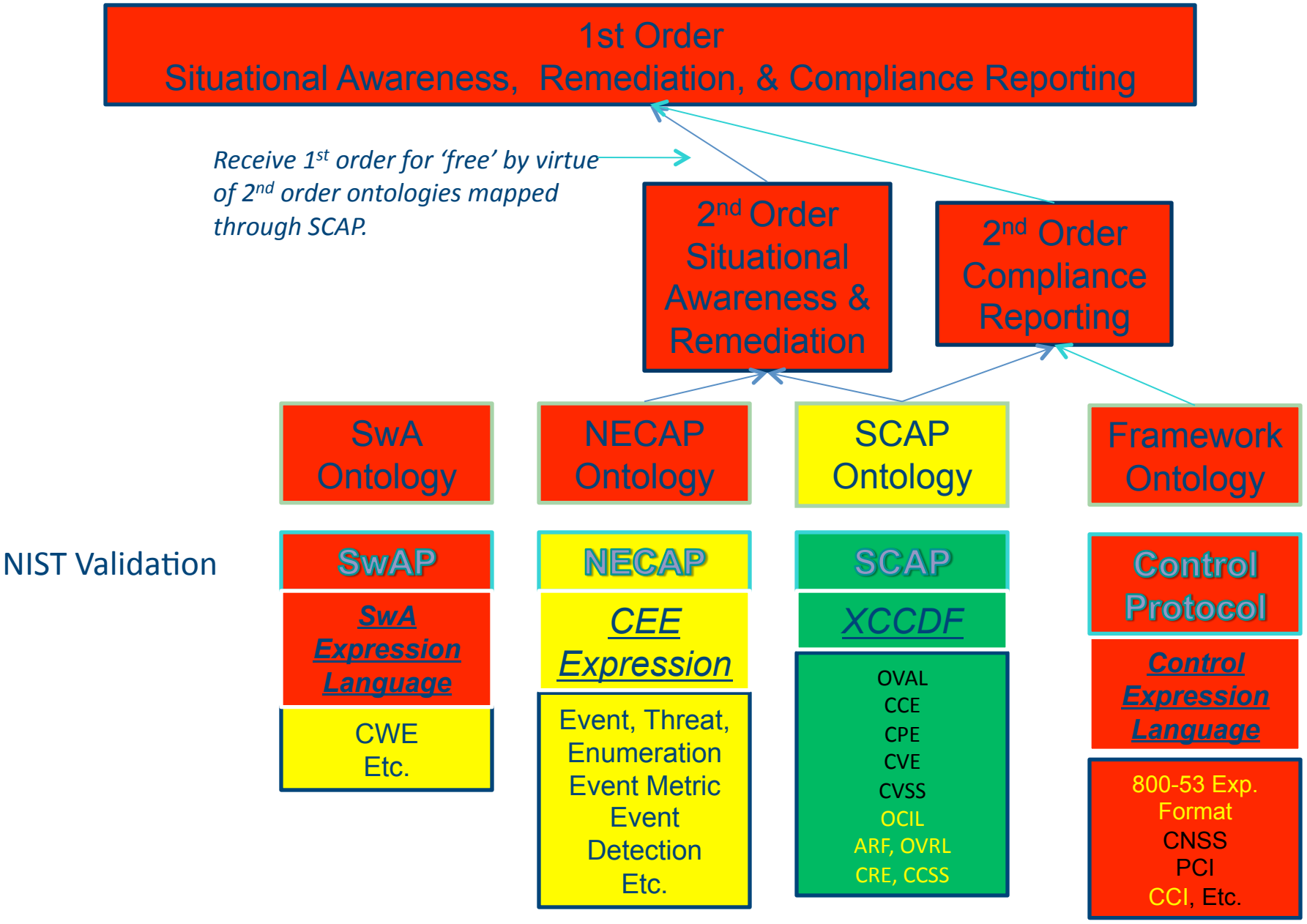
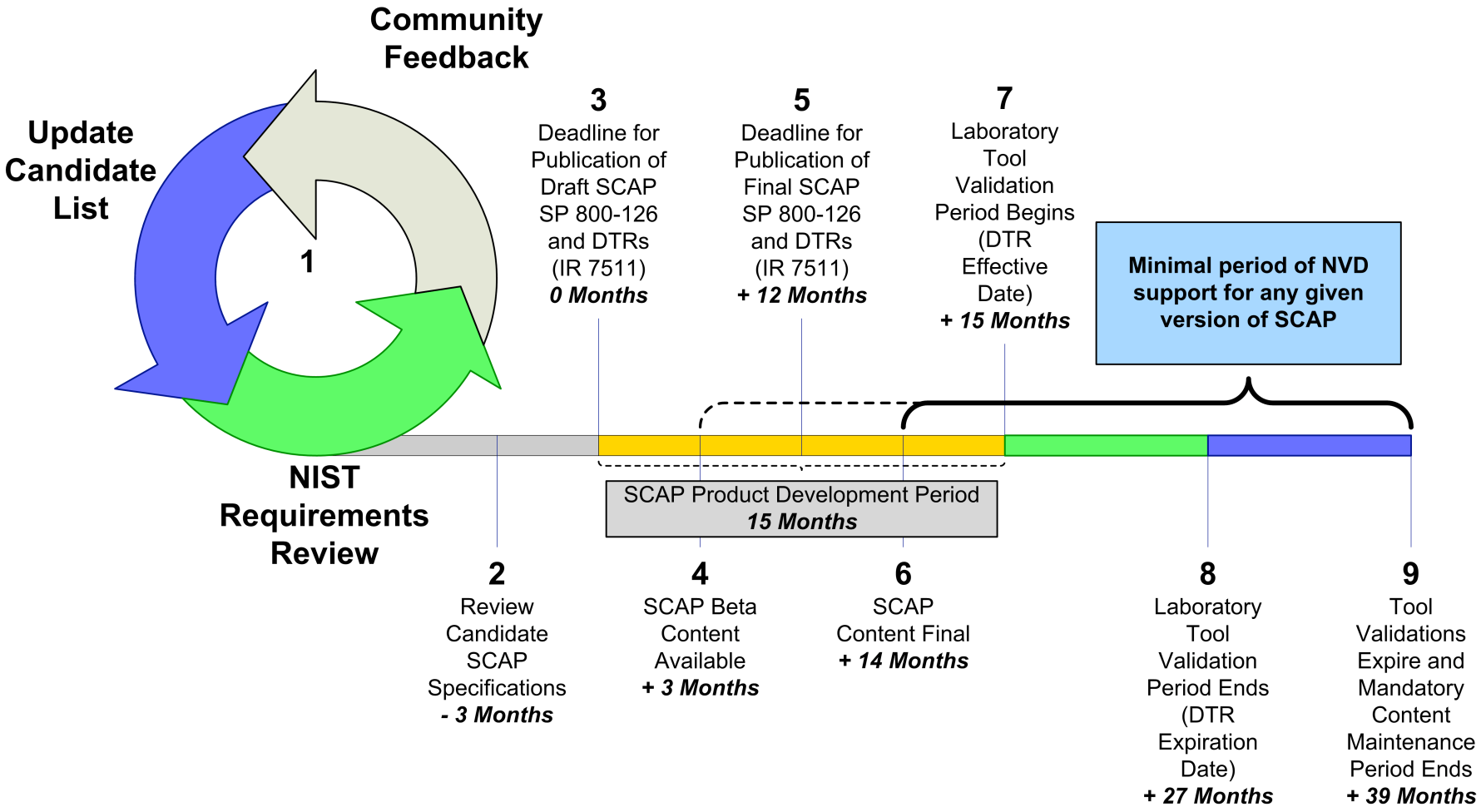
Security Content Automation Protocol Lifecycle and Documents Overview

presented by:
John Banghart

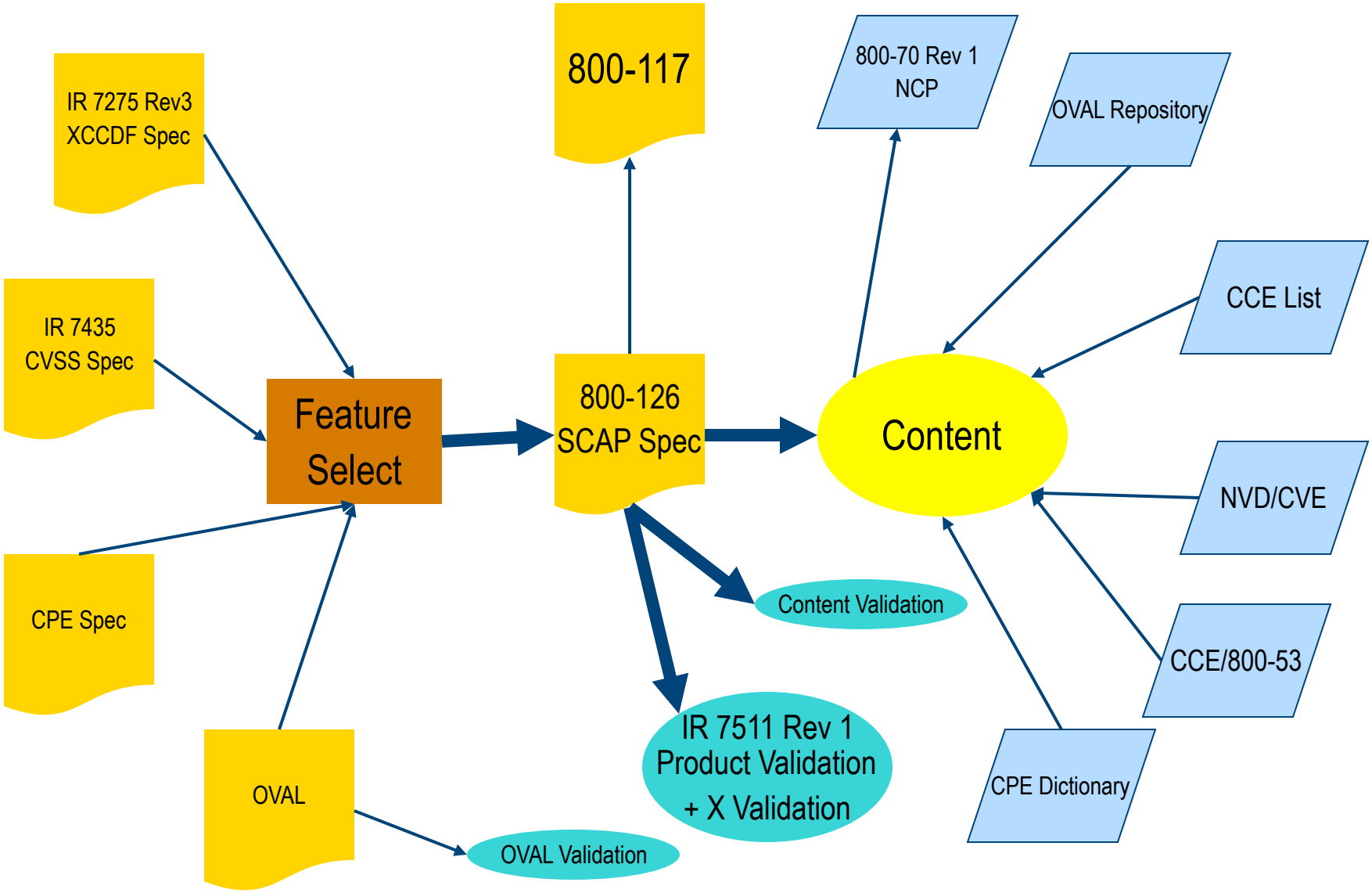
Security Automation (Current State)



SCAP Lifecycle



Document and Data Relationships



Emerging Specifications

http://scap.nist.gov/emerging-specs/index.html

- To be considered for NIST Validation
  - Be in final specification format.
  - Address use cases that are consistent with the SCAP vision and provide value and utility to the SCAP community.
  - Demonstrate a high degree of maturity.
  - Demonstrate uptake and adoption by product vendors, agencies, and organizations.
  - Demonstrate interoperability with existing SCAP component specifications.
  - Have a specification submission that is accompanied by a functioning reference implementation.
  - Have a specification submission that includes evidence of public vetting (mailing lists, workshops, etc.)
  - Be operationally used in organization(s) as a pilot or full operations.
  - Be free from proprietary claims of intellectual property.

Community Next Steps

- Take Part in Community Discussions
- Develop and Use SCAP Validated Products
- Publish Security Configurations in SCAP Format and Consider Whether Those Security Configurations Are Well-Suited for The National Checklist Program
- Extend SCAP Use Cases
  - Processing signed content

Questions?

Presenter:

John Banghart

john.banghart@nist.gov

SCAP Homepage: http://scap.nist.gov

National Checklist Program: http://checklists.nist.gov

National Vulnerability Database: http://nvd.nist.gov

Lifecycle Step 1

- **The NIST review, community feedback, and update candidate process** - This step allows a specification to mature and demonstrate value in terms of operational use within organizations, community feedback, vendor use and adoption, etc., without imposing a time limit.

Lifecycle Step 2

- **Review Candidate SCAP Specifications** - As specifications evolve, NIST may consider a new or modified specification for SCAP adoption. Periodically, a specification reaches a degree of maturity, adoption, and utility where NIST considers it a potential candidate for SCAP. These specifications will be announced so that the community will have time to provide additional comments and feedback before the specification becomes final. If the specification is already final, this will allow an additional comment period before NIST publishes the draft NIST SP 800-126 (see step 3).

Lifecycle Step 3

- **Deadline for Publication of Draft SCAP SP 800-126 and Validation DTRs (NIST IR 7511)** - Candidate specifications that are identified as potential SCAP specifications will be included in the Draft NIST SP 800-126. Likewise, a draft publication of NIST IR 7511: *Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements* will be updated to include derived test requirements (DTRs). These draft publications serve as the official notice to the community that the validation testing program will include new or updated specifications. If there are no new candidate specifications and there are no changes to the specifications from the previous year, then the current NIST SP 800-126 will remain in effect. Review of this draft will follow the NIST publication review process.

Lifecycle Step 4

- **SCAP Beta Content Available** - After publishing the draft NIST SP 800-126 and NIST IR 7511, NIST will provide sample, beta quality content, for data streams for which they are responsible. For example, NIST is currently the custodian of the FDCC SCAP content on behalf of OMB. If the NIST SP 800-126 includes a new specification that will affect the FDCC SCAP content, beta FDCC SCAP content will be produced by NIST for use/testing by the community.

Lifecycle Step 5

- **Deadline for Publication of Final NIST SP 800-126 and Validation DTRs (NIST IR 7511)** - No later than twelve months after the draft NIST SP 800-126 and NIST IR 7511 are published, they will become effective.

Lifecycle Step 6

- **SCAP Content Final** - Related to step 4, content originally published as beta will become final at this time. The community can expect that the content will be released in various maturing versions including several versions of alpha, several versions of beta, and then in a final version at this time.

Lifecycle Step 7

- **Laboratory Product Validation Period Begins (DTR Effective Date)** - After the finalization of NIST SP 800-126 and NIST IR 7511, accredited laboratories begin testing products using the finalized SP 800-126 and IR 7511 as official references. Products seeking new validations and those seeking re-validations will be tested using these new or updated documents. Even if the NIST SP 800-126 does not change, re-validation may be necessary due to changes in the NIST IR 7511.

Lifecycle Step 8

- **Laboratory Product Validation Period Ends (DTR Expiration Date)** - 12 months from the start of step 7, product testing according to the previous versions of NIST SP 800-126 and NIST IR 7511 ends. Future product testing will use the latest versions of NIST SP 800-126 and NIST IR 7511.

Lifecycle Step 9

- **Product Validations Expire and Mandatory Content Maintenance Period Ends** - Product validations are valid for 1 year from the time the validation was originally awarded. As a result, there will be overlapping validations adhering to different versions of NIST SP 800-126 and NIST IR 7511. NIST will maintain all SCAP content for a minimum period of 12 months from the date of step 8. As a general practice NIST maintains content using the "least version principle" to insure a maximum amount of backwards compatibility.

SCAP Documentation

- **SP800-117**: Adopting and Using Security Content Automation Protocol
- **SP800-126**: Security Content Automation Protocol Specification
- **SP800-70 Rev 1**: DRAFT National Checklist Program for IT Products--Guidelines for Checklist Users and Developers
- **IR-7511**: DRAFT Security Content Automation Protocol (SCAP) Validation Program Test Requirements
- **IR-7435**: The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems
  IR-7275 Rev 3: Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4

SP800-126: Security Content Automation Protocol Specification

- SP800-126 defines the technical specification for version 1.0 of the Security Content Automation Protocol (SCAP). SCAP (pronounced S-CAP) comprises a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. This document describes the basics of the SCAP component specifications and their interrelationships. It also defines the characteristics of SCAP content, as well as all other requirements for SCAP that are not defined in the individual SCAP component specifications. This guide provides recommendations on how to leverage SCAP to achieve security automation for organizations seeking to implement SCAP.

SP800-117: Adopting and Using Security Content Automation Protocol

- **Purpose and Scope**: SP 800-117 provides an overview of SCAP, focusing on how organizations can use SCAP-enabled tools to enhance their security posture. It also explains how IT product and service vendors can adopt SCAP's capabilities within their offerings.
- **Audience**: Individuals who have responsibilities for maintaining or verifying the security of systems in operational environments. This includes mid-level management, chief information security officers, and technical directors within Federal and state governments and other large organizations; software and hardware vendor product managers, and auditors.

SP800-70 Rev 1: DRAFT National Checklist Program for IT Products--Guidelines for Checklist Users and Developers

- **Purpose and Scope**: 800-70 Rev 1 describes security configuration checklists and their benefits, and it explains how to use the NIST National Checklist Program (NCP) to find and retrieve checklists. The publication also describes the policies, procedures, and general requirements for participation in the NCP.
- **Audience**: current and potential checklist developers and users in both the public and private sectors. Checklist developers include information technology (IT) vendors, consortia, industry, government organizations, and others in the public and private sectors. Checklist users include end users, system administrators, and IT managers within government agencies, corporations, small businesses, and other organizations, as well as private citizens.

IR-7511 Rev 1: DRAFT Security Content Automation Protocol (SCAP) Validation Program Test Requirements

- **Purpose and Scope**: IR-7511 Rev 1 describes the requirements that must be met by products to achieve SCAP Validation. Validation is awarded based on a defined set of SCAP capabilities and/or individual SCAP components by independent laboratories that have been accredited for SCAP testing by the NIST National Voluntary Laboratory Accreditation Program. **Audience**: Laboratories that are accredited to do SCAP product testing for the program, vendors that are interested in receiving SCAP validation for their products, and government agencies and integrators seeking to deploy SCAP tools in their environments.

IR-7435: The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems

- **Purpose and Scope**: IR-7435 describes the Common Vulnerability Scoring System (CVSS) which provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

IR-7275 Rev 3: Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4

- **Purpose and Scope**: IR-7275 Rev 3 specifies the data model and Extensible Markup Language (XML) representation for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4. It is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. It also defines a data model and format for storing results of security guidance or checklist compliance testing.
- **Audience**: Government and industry security analysts, and industry security management product developers.

Extending the SCAP Domain Vocabulary

Candidate Domains

- Incidents
- Events
- Threats
- Remediation/Countermeasures
- Networks
- Performance Data

Extending Vocabulary

- Define information security ontologies which express common terms and relationships, and provide reasoning and inference capabilities
- Publish web services built upon SCAP core enumerations and languages