FDCC/USGCB

- **2006 – 2014 Federal Desktop Core Configuration & United States Govt. Configuration Baseline**

- **What is FDCC/USGCB?**

  OMB initiative to provide mandatory/uniform configurations for commonly used operating systems and applications

  FDCC Policy memos (M-07-11, M-08-22, CIO Council Memos, etc.)

- **NIST Checklists (FAR section 39.101, Paragraph d)**

- **How are FDCC & USGCB related**

- **Why NIST?**

  National Checklist Program

  Security Content Automation Protocol (SCAP)

  Leveraging existing processes & open process

FDCC & USGCB (continued)

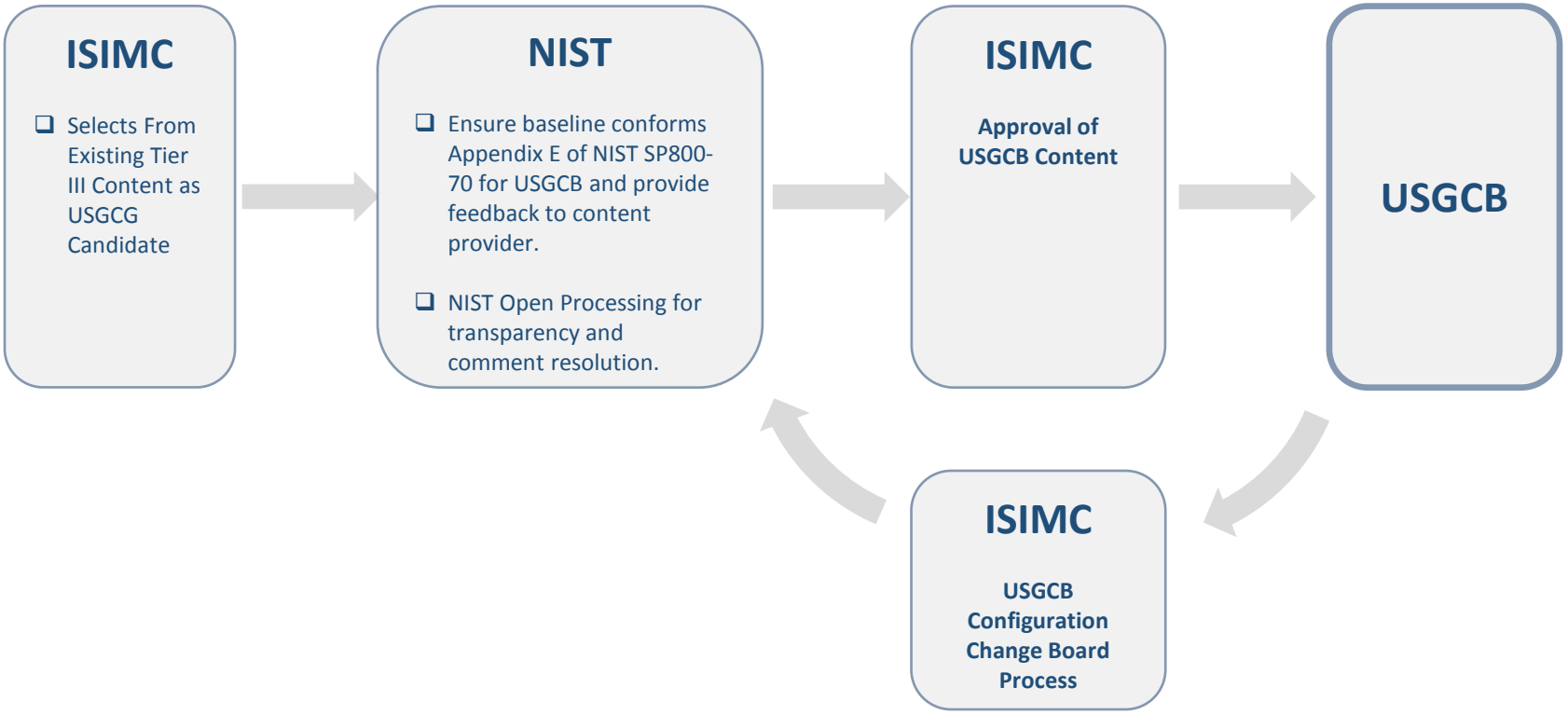
- **The Target Configuration Moved…**
  - *FDCC - Specialized Security-Limited Functionality*
  - *USGCB - Enterprise-level security*
  - *Which was more successful?*

- **FDCC - More than just configuration settings…**
  - *Vendor self assertion (M-08-22)*
  - *Mandatory FISMA reporting (M-14-04, etc.)*
  - *Identifies NIST NCP as required configurations for all federal agencies when purchasing (FAR section 39.101, Paragraph d)*

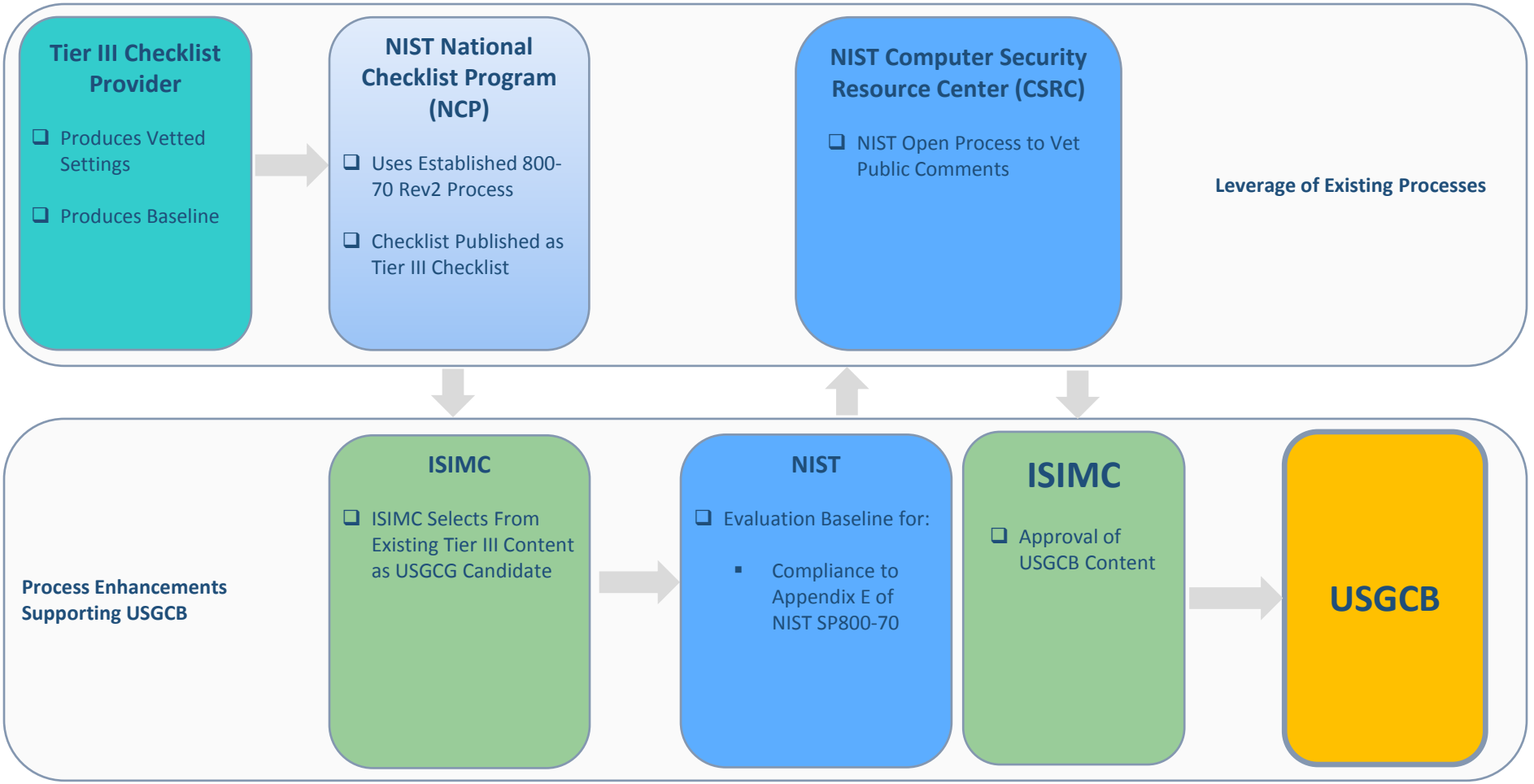
Is There Real Value?

- Over 30 agencies/organizations asking for more
- Conficker, USB, etc.
- Assessment/Audit teams
- Know the extent of compromise
- FIPS 140 compliance, etc.
- FISMA compliance
- SANS top 20

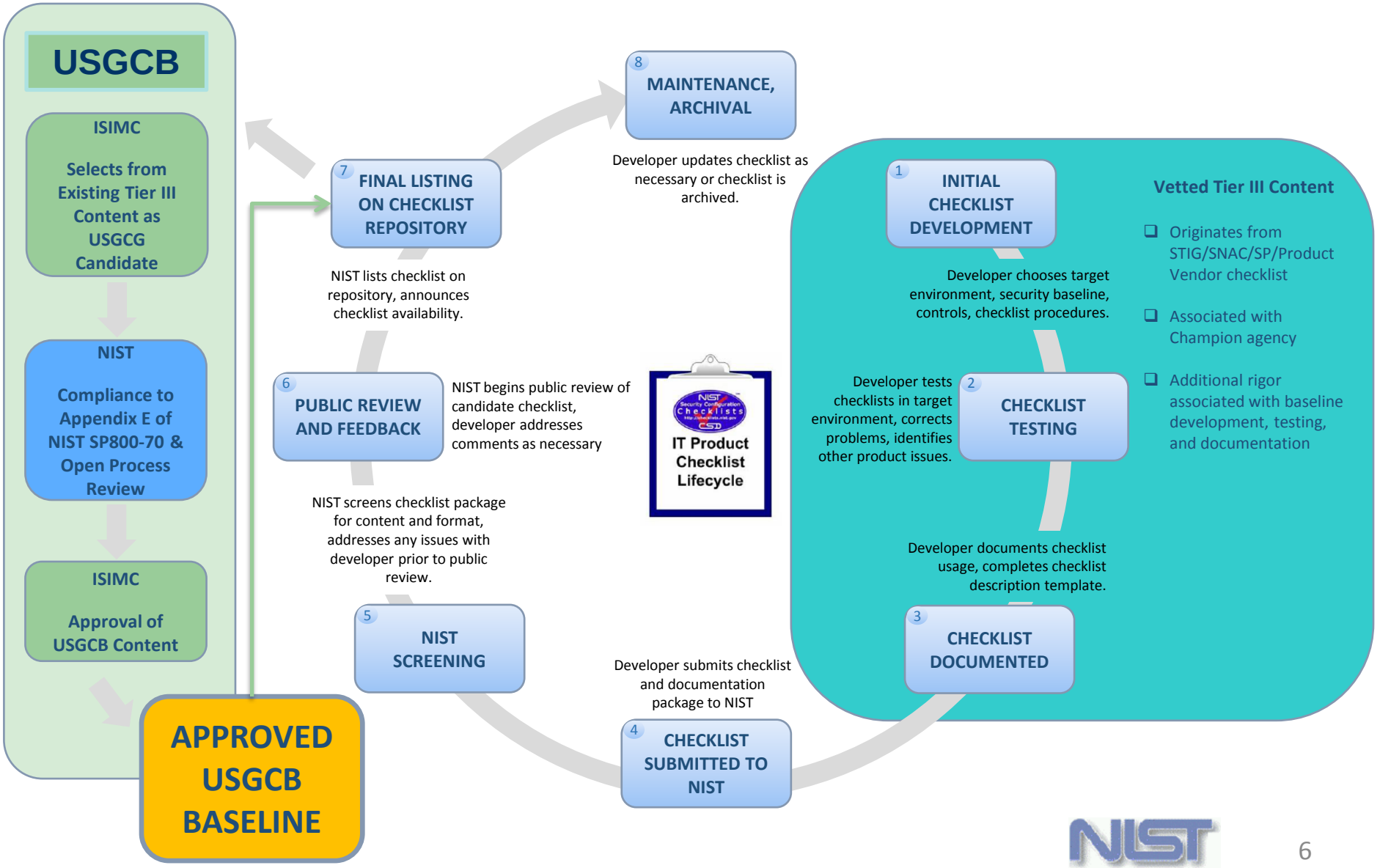
ISIMC USGCB Process (10,000 Foot View)



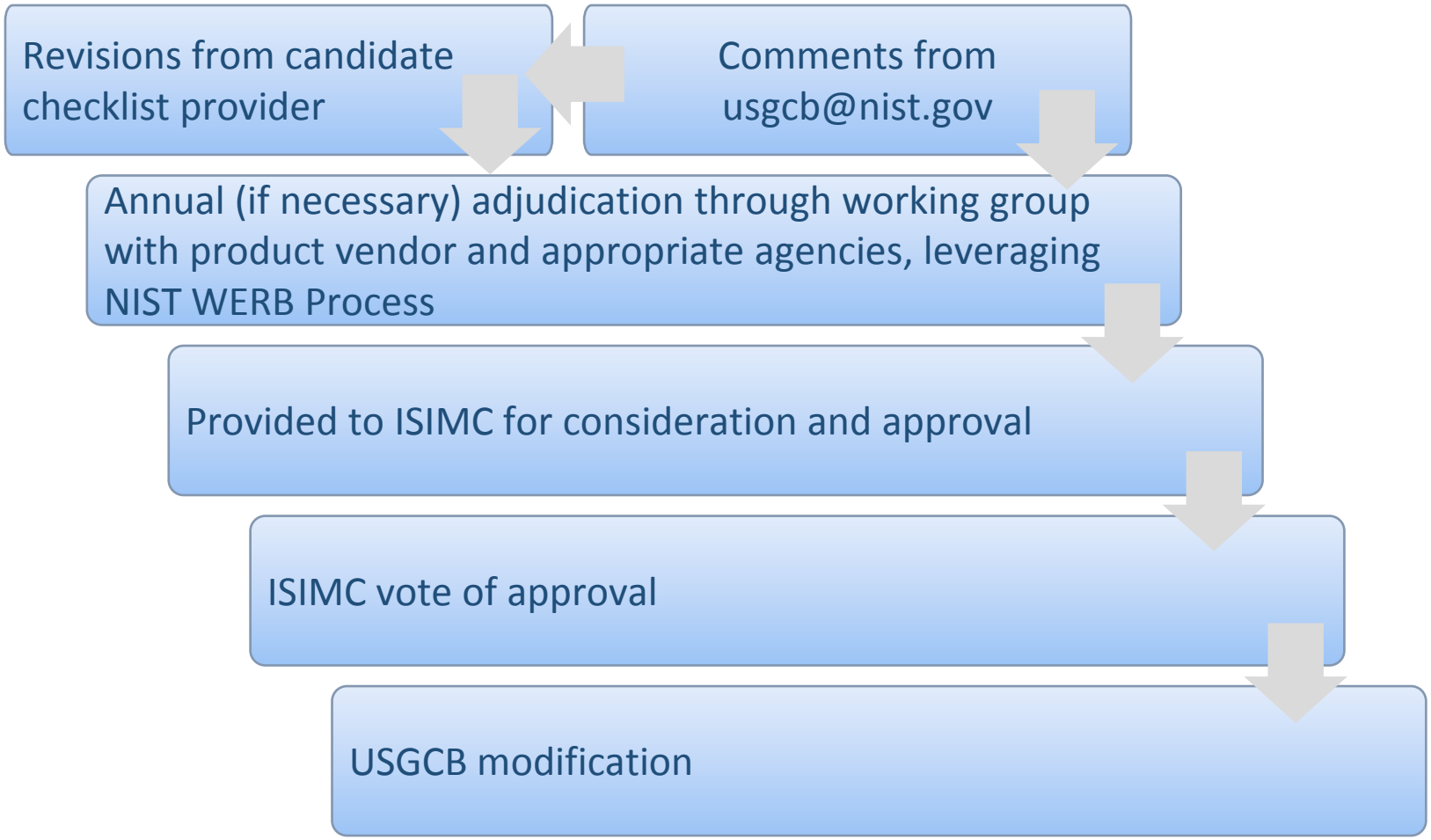
Full USGCB Process



Full USGCG Process/SP800-70 Overlay



ISIMC USGCB CCB Process



References

- **NIST Special Publications**
  - *SP800-70* http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf
  - *SP800-117* http://csrc.nist.gov/publications/nistpubs/800-117/sp800-117.pdf
  - *SP800-126* http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf
- **NIST Interagency Reports**
  - *NIST IR 7511 Rev. 3* http://csrc.nist.gov/publications/drafts/nistir-7511/Draft-nistir-7511_R3.pdf
- **DISA STIGs** http://iase.disa.mil/stigs/Pages/index.aspx
- **NSA Security Configuration Guides**
  https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml
- **OMB Memoranda**
  - *M-07-11* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-11.pdf
  - *M-08-22* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-22.pdf
- **FAR** https://acquisition.gov/far/

Supplemental Information

The following supplemental slides describe:

- SCAP content authorship and testing limitations
- SCAP Validated Products
- SCAP Product Validation Limitations
- What's new in SCAP & the NCP

SCAP Content

- SCAP content authorship has been assumed by product vendors, open working groups, and other government agencies (i.e. DISA) with operational responsibilities.

- NIST conducts SCAP content validation for syntactic compliance to the SCAP specifications as part of the National Checklist Program as defined in NIST SP800-70, which differs from semantic testing of SCAP content.

- Although semantic testing is the responsibility of content authors, correction of semantic errors is governed by the NIST800-70 Appendix D agreement between NIST and the content authors.

SCAP Content (cont.)

- **USGCB SCAP content semantic testing is conducted external to NIST in four phases:**
  1) *Before SCAP content is submitted to the National Checklist Program;*
  2) *During the NCP public comment period of the content;*
  3) *During the formal CSRC NIST Public Comment period ; and,*
  4) *Continuously through agency/organization O&M use of the content with feedback to the NIST National Checklist Program to broker error correction through the NCP.*

- **NIST is updating Appendix E of SP800-70 to reflect the aforementioned bullets**

SCAP Validated Products

- **SCAP 1.0 Product Validation Have Expired.**

  It is likely that new USGCB designations will not work in products with expired SCAP 1.0 product validations for several reasons including: USGCB candidates will be selected from Tier III checklists that have SCAP versions greater than the SCAP 1.0 version (i.e. SCAP 1.1, SCAP 1.2).

- **Although SCAP 1.2 validated products have been tested to ensure backward compatibility for processing SCAP 1.0 content, the SCAP 1.2 validation program's battery of tests concentrated more heavily on the feature set of SCAP 1.2.**

SCAP 1.2 Validated Products

- BMC Client Management 12.0.0
- McAfee Policy Auditor 6.2
- Red Hat OpenSCAP 1.0.8
- CIS Configuration Assessment Tool 3
- Tripwire Enterprise 8

What's New

- **SCAP Validation Program 1.2 (previous 1.0 expired)**

  Lesson Learned: Ensure higher degree of Content Product Interoperability Assurance

  Predictive Interoperability: Bigger & Better Covers 45 of 146 total OVAL test types (all the popular ones) (NIST IR 7511 Rev. 3)

  SCAP Content Validation (SCAPVal)

- **SCAP Adoption**

  58 New Tier III SCAP Data Streams (currently in NCP)

  New automated production and editing tools

  - Red Hat OpenSCAP
  - Microsoft XTrans
  - DISA DPMS
  - G2 eSCAPe, RATEL
  - Tresys SCC
  - Others…

- **Additional Use Cases**

  Advance Persistent Threats (APT) OS Features (i.e. EMET)

  Vendor supported SCAP to morph in face of attack

  APT Detection using SCAP