
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)

- **ISIMC**
  - Selects From Existing Tier III Content as USGCG Candidate

- **NIST**
  - Ensure baseline conforms Appendix E of NIST SP800-70 for USGCB and provide feedback to content provider.
  - NIST Open Processing for transparency and comment resolution.

- **ISIMC**
  - Approval of USGCB Content

- **USGCB**

- **ISIMC**
  - USGCB Configuration Change Board Process
Full USGCB Process

Tier III Checklist Provider
- Produces Vetted Settings
- Produces Baseline

NIST National Checklist Program (NCP)
- Uses Established 800-70 Rev2 Process
- Checklist Published as Tier III Checklist

NIST Computer Security Resource Center (CSRC)
- NIST Open Process to Vet Public Comments

Leverage of Existing Processes

ISIMC
- ISIMC Selects From Existing Tier III Content as USGCG Candidate

NIST
- Evaluation Baseline for:
  - Compliance to Appendix E of NIST SP800-70

ISIMC
- Approval of USGCB Content

USGCB

Process Enhancements Supporting USGCB
Developer submits checklist and documentation package to NIST.

NIST begins public review of candidate checklist, developer addresses comments as necessary.

NIST screens checklist package for content and format, addresses any issues with developer prior to public review.

NIST lists checklist on repository, announces checklist availability.

Developer updates checklist as necessary or checklist is archived.

ISIMC Selects from Existing Tier III Content as USGCG Candidate

NIST Compliance to Appendix E of NIST SP800-70 & Open Process Review

ISIMC Approval of USGCB Content

FULL USGCG PROCESS/SP800-70 OVERLAY

VETTED TIER III CONTENT

- Originates from STIG/SNAC/SP/Product Vendor checklist
- Associated with Champion agency
- Additional rigor associated with baseline development, testing, and documentation

DEVELOPMENT

- Developer chooses target environment, security baseline, controls, checklist procedures.
- Developer tests checklists in target environment, corrects problems, identifies other product issues.
- Developer documents checklist usage, completes checklist description template.

DOCUMENTED

- Developer submits checklist and documentation package to NIST
- NIST lists checklist on repository, announces checklist availability.

SUBMITTED TO NIST

- NIST screens checklist package for content and format, addresses any issues with developer prior to public review.

SCREENING

- NIST begins public review of candidate checklist, developer addresses comments as necessary

REPOSITORY

- NIST lists checklist on repository, announces checklist availability.

PUBLIC REVIEW AND FEEDBACK

- NIST screens checklist package for content and format, addresses any issues with developer prior to public review.

LIBRARY

- NIST lists checklist on repository, announces checklist availability.

FINAL LISTING ON CHECKLIST REPOSITORY

- NIST lists checklist on repository, announces checklist availability.

MAINTENANCE, ARCHIVAL

- Developer updates checklist as necessary or checklist is archived.

APPROVED USGCB BASELINE
Comments from usgcb@nist.gov

Annual (if necessary) adjudication through working group with product vendor and appropriate agencies, leveraging NIST WERB Process

Provided to ISIMC for consideration and approval

ISIMC vote of approval

USGCB modification
References

- **NIST Special Publications**

- **NIST Interagency Reports**

- **DISA STIGs** [http://iase.disa.mil/stigs/Pages/index.aspx](http://iase.disa.mil/stigs/Pages/index.aspx)

- **NSA Security Configuration Guides**

- **OMB Memoranda**

- **FAR** [https://acquisition.gov/far/](https://acquisition.gov/far/)
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.
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*