

## NIST HANDBOOK 150-17 Annex E CHECKLIST

### Security Content Automation Protocol Testing

**Instructions to the Assessor:** This checklist addresses specific accreditation requirements prescribed in NIST Handbook 150-17, *Cryptographic and Security Testing*, for the Security Content Automation Protocol Testing test methods. It is used in conjunction with the NIST Handbook 150-17 Checklist, which covers the requirements in clauses 4 and 5 of the program handbook.

Place an "X" beside any of the following items that represent a nonconformity. Place a "C" beside each item on which you are commenting for other reasons. Record the item number and your nonconformity explanation and/or comments on the appropriate comment sheet(s). Write "OK" beside all other items you observed or verified as compliant at the laboratory.

**Note:** The numbering of the checklist items correlates to the numbering scheme in NIST Handbook 150-17, Annex E, Section E.5.

#### E.5 Additional technical requirements for accreditation

##### E.5.2 Additional personnel requirements

— The laboratory shall demonstrate, in addition to the technical expertise required by each test method as described below, that their personnel has basic knowledge of cryptographic and security practice for information systems and that the laboratory is aware of the governing standards and publications, especially the ones listed in this handbook.

The laboratory's personnel shall have experience, training, basic knowledge, or familiarity in:

- a) vulnerability and configuration management (NIST SP 800-40 v2 or later and NIST SP 800-100);
- b) XML and how to read XML documents (W3C Extensible Markup Language (XML) 1.1 (Second Edition) or later);
- c) all SCAP specifications (XCCDF, OVAL, OCIL, CVE, CCE, CPE, CCSS, CVSS, Asset Identification, ARF, and TMSAF, including NIST SP 800-126) – latest versions (for more information see <http://scap.nist.gov>); and
- d) the Windows XP, Windows Vista, Windows 7, and Red Hat Enterprise Linux operating systems.

---

**E.5.3 Additional accomodation and environmental conditions**

— The laboratory shall have appropriate areas, including ventilation and safety, for the use of test methods using chemical solvents and heating/cooling apparatus.

**E.5.5 Additional equipment requirements**

— The laboratory shall be equipped with the following minimum hardware, software, and operating system requirements:

**a) Hardware:**

- 1) Any IT system capable of properly executing Red Hat Enterprise Linux 5 Desktop, Windows XP SP 3, Windows Vista SP2, Windows 7 SP1, and a domain controller such as Windows Server.

**b) Software:**

- 1) Windows XP SP3, Windows Vista SP2, and Windows 7 SP1 running on the IT system.
- i. The operating system must be configured according to the configuration requirements in the Implementation Guide.
  - ii. The OS must have Internet Explorer version 7 installed on Windows XP and Vista, and Internet Explorer version 8 on Windows 7.
  - iii. The OS must be able to be joined to a test domain.
- 2) Red Hat Enterprise Linux 5 Desktop running on the IT system.
- i. The operating system must be configured according to the configuration requirements in the Implementation Guide.
- 3) XML schema validation tool.
- 4) SCAP Reference Implementation - Requires Java Runtime Environment (JRE) version 1.5 or later.
- 5) XML viewer.
- 6) Access to the official NIST CVSS calculator, located at <http://nvd.nist.gov/cvss.cfm?calculator&version=2>.
- 7) Access to the National Vulnerability Database at <http://nvd.nist.gov>.

