NVLAP®	**DEPARTMENT OF COMMERCE** National Institute of Standards and Technology National Voluntary Laboratory Accreditation Program	**ISSUE DATE:** May 14, 2013
	LAB BULLETIN	**NUMBER:** LB-74-2013
		LAP: Cryptographic and Security Testing
SUBJECT: Revision of SCAP Testing to the NVLAP Cryptographic and Security Testing Laboratory Accreditation Program		

Revision of NIST Handbook 150-17 to incorporate revised SCAP test methods

At the request of the NIST Security Content Automation Protocol (SCAP) Validation Program, NVLAP announces the revision of NIST Handbook 150-17 to incorporate revised SCAP test methods to the NVLAP Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP). These revised methods incorporate SCAP version 1.2, which is comprised of eleven component specifications:

- eXtensible Configuration Checklist Description Format (XCCDF) – a standard XML for specifying checklists
- Open Vulnerability and Assessment Language (OVAL) – a standard XML for checking the machine state
- Open Checklist Interactive Language (OCIL) – a language for representing checks that collect information from people or from existing data stores made by other data collection efforts
- Common Vulnerabilities and Exposures (CVE) – a dictionary of security-related software flaws
- Common Configuration Enumeration (CCE) – a dictionary of software misconfigurations
- Common Platform Enumeration (CPE) – a standard nomenclature and dictionary for product naming
- Common Configuration Scoring System (CCSS) – a standard for measuring the relative severity of system security configuration issues
- Common Vulnerability Scoring System (CVSS) – a standard for scoring the impact of vulnerabilities
- Asset Identification – a format for uniquely identifying assets based on known identifiers and/or known information about the assets
- Asset Reporting Format (ARF) – a format for expressing the transport format of information about assets and the relationships between assets and reports
- Trust Model for Security Automation Data (TMSAD) – a specification for using digital signatures in a common trust model applied to other security automation specifications.

For additional technical information regarding these test method revisions, contact the SCAP Program Manager, Melanie Cook, at melanie.cook@nist.gov, 301-975-5259.

The NVLAP Program-Specific Handbook for the CST LAP, NIST Handbook 150-17, has been revised to incorporate these changes and was published on May 9, 2013. As of the date of this bulletin, NVLAP will begin accepting applications for accreditation from any laboratory that meets the requirements of NIST Handbook 150, *NVLAP Procedures and General Requirements*, NIST Handbook 150-17, *Cryptographic and Security Testing* (Sections 4 and 5 and Annex E), and the technical requirements for the testing prescribed by SCAP. To view and download NIST Handbook 150:2006 and NIST Handbook 150-17:2013, see: http://www.nist.gov/nvlap.

Conditions for a laboratory already accredited for SCAP test methods in the CST LAP to apply for addition of revised SCAP methods to its scope of accreditation

In order for a laboratory already accredited in the CST LAP to add the SCAP 1.2 test methods to its scope of accreditation, the laboratory must:

1. Request expansion of the scope of accreditation for SCAP 1.2 testing, in writing, by submitting the completed program-specific application pages **by June 30, 2013**;

2. Provide management system documentation to NVLAP, including the procedures and instructions written to conduct SCAP 1.2 testing, with the expansion request;

3. Schedule to undergo a technical assessment by NVLAP via teleconference **by July 31, 2013**; and

4. Provide a corrective action response(s) along with supporting objective evidence for resolving any nonconformities identified.

Please note that laboratories with an existing scope of accreditation that includes SCAP testing may continue to conduct tests for the SCAP methods and provide submission of testing results to the NIST SCAP Validation Program.

Questions concerning the SCAP accreditation procedures should be directed to Dana Leaman, dana.leaman@nist.gov, 301-975-4679.