NVLAP®	**DEPARTMENT OF COMMERCE** National Institute of Standards and Technology National Voluntary Laboratory Accreditation Program	**ISSUE DATE:** June 21, 2013
	LAB BULLETIN	**NUMBER:** LB-77-2013
		LAP: Cryptographic and Security Testing

SUBJECT: Addition of New Requirements to NIST Handbook 150-17 Regarding Use of FIPS 140-2 Validated Cryptography

The purpose of this bulletin is to publish a minor revision to NIST Handbook 150-17 for each of the subclauses noted below. This bulletin becomes a part of NIST Handbook 150-17, *Cryptographic and Security Testing*, until such time as the next edition of the handbook is published.

Overview

NIST Handbook 150, 4.1.5 c) outlines the general requirement for an accredited laboratory regarding the protection of its customers' confidential information. More specifically, in NIST Handbook 150-17, clauses 4.4.2, 4.13.1.4, 4.13.2.1, and 5.10.3.2 address specific requirements that pertain to how laboratories accredited in the program protect confidential information. At the request of the NIST Cryptographic Module Validation Program (CMVP) and the Canadian Communications Security Establishment Canada (CSEC), NVLAP has revised NIST Handbook 150-17 to require use of Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules when cryptography is employed in the protection of information.

Background

FIPS 140-1 became a mandatory standard for the protection of sensitive data when the Secretary of Commerce signed the standard on January 11, 1994. FIPS 140-2 superseded FIPS 140-1 when the standard was signed on May 25, 2001.

FIPS 140-2 precludes the use of unvalidated cryptography for the cryptographic protection of sensitive or valuable data within federal systems. Unvalidated cryptography is viewed as providing no protection to the information or data – in effect the data would be considered unprotected plain text.

Implementation of changes

Effective upon the issuance of this bulletin, the following clauses of NIST Handbook 150-17 are revised as shown in the italicized text:

1) 4.4.2 Policies for documents storage and maintenance of contracts under confidentiality, nondisclosure agreements, marked as secret, or copyright protected, shall be well defined according to the document's status. These documents shall be protected commensurate with their classification and/or sensitivity, and access to them shall be given only to authorized personnel.

When cryptography is utilized as the mechanism for protection of information, the cryptographic module used shall be FIPS 140-2 validated.

2) 4.13.1.4 Records of all management system activities including training, internal audits, and management reviews shall be securely saved for future reviews. The integrity of electronic documents shall be assured by means commensurate with the data sensitivity. *When cryptography is utilized as the mechanism for protection of information, the cryptographic module used shall be FIPS 140-2 validated.* Documents in hard copy form shall be marked and stored in a secure location and, if necessary, a file logging any access, change, or addition shall be maintained to preserve a document's integrity and prevent unauthorized changes.

3) 4.13.2.1 The final test results and/or the test reports generated using cryptographic or security testing tools for the IUT or SUT shall be kept by the laboratory following the completion of testing for the life of the IUT or SUT, or as specified by the validation body and/or vendor in writing. Records may include hard or digital copies of the official test results and the test results error file(s). Records shall be stored in a manner that assures survivability, confidentiality, integrity, and accessibility. *When cryptography is utilized as the mechanism for protection of information, the cryptographic module used shall be FIPS 140-2 validated.*

4) 5.10.3.2 The laboratory shall ensure that an integrity and confidentiality mechanism commensurate with the data sensitivity and/or programmatic requirements and/or government requirements when electronic delivery of the test reports to the validation program is employed to ensure that the test report cannot be disclosed to anyone other than the intended recipient(s) and an integrity mechanism exists to ensure that the test report is not modified. *When cryptography is utilized as the mechanism for protection of information, the cryptographic module used shall be FIPS 140-2 validated.*

During a laboratory's next on-site assessment, the laboratory will be assessed against these revised requirements. Any noncompliance with the revised requirements will be reported as a nonconformity.

Questions regarding the changes to the NVLAP CST LAP requirements should be directed to Dana Leaman, dana.leaman@nist.gov, 301-975-4679.