

FIPS 140-3
Cryptographic Module Validation Program
Management Manual

(Date 05/07/2025)

Version 2.4

National Institute of Standards and Technology and
Canadian Centre for Cyber Security

Revision History

Version	Date	Comment
1.0	9/21/2020	First draft release for FIPS 140-3 program
1.1	7/13/2022	Second draft release. Major rewrite.
1.2	12/23/2022	Third draft release. Updates to address feedback submitted July 2022.
2.0	12/06/2023	Final version. Updates to address feedback submitted February 2023 and final review comments.
2.1	02/29/2024	4.4.6 (Changes while in Coordination): Provided new options and guidance for changes while in Coordination. 7.1.15 (Additional Comments): 1 and 2 were clarified when Security Levels are changed.
2.2	04/19/2024	3.2.8 (Suspension, Denial and Revocation of Accreditation): Added “Quality errors” into the second points category. 4.4.5 (Resubmission while in Review Pending) & 4.4.6 (Changes while in Coordination): Small clarifications. 4.8 (Validation Revocation or Historical): Clarified Revocation and Historical guidance. 7.1 (Submission Scenarios): Minor grammatical / typographical corrections.
2.3	12/17/2024	General clean up (e.g., grammar, formatting, references, navigation including changing all “shall” to “must” outside of Section 7 for consistency). 2.4 (CMVP Points of Contact): Added email categories for general or CSTL usage. 2.5.2 (Request for Guidance Format): Updated RFG Template and added reference to IG template. 3.2.4 (Relocation of a CSTL): Customer ID may change if change in location. 3.2.8 (Extended Cost Recovery): Significant revision to remove duplication and reduce ambiguity by specifying ECR categories with examples in a new table. 3.2.9 (Suspension of Accreditation): Revised text around

		<p>suspension.</p> <p>4.3.3 (Request for Transition Period Extension): New section.</p> <p>6.2 (Suggested Tools for Physical Testing): Added text in the first paragraph around calibration and a few other minor changes.</p> <p>7.1.1 (Requirements for all revalidations): Updated guidance for new CSTLs.</p> <p>7.1.2.1 (Interim Validation): New section.</p> <p>7.1.5 (Non-Security Relevant (NSRL)): Added ‘d’ on minimum test requirements.</p> <p>7.8 (Module definitions for same certificates): Added “self-tests”.</p>
2.4	05/07/2025	<p>General: minor formatting, non-technical content and reference updates.</p> <p>1.2 (Purpose of the CMVP Management Manual): merged content with section 1.3 (Applicability and Scope).</p> <p>1.5 (Use of Validated Products): merged content with content from the CMVP webpage.</p> <p>7.1.10 (Update (UPDT)): Allow UPDT to combine with VUP and VAOE.</p> <p>7.1.14 (Submission Scenario Summary Table): Added “Code changes” and “CAVP” columns and footnotes.</p> <p>7.2.1. (Vendor Affirmation of Security Functions and Methods): some formatting changes and corrections to outdated/incorrect text.</p> <p>7.4 (Remote Testing of Modules): Editorial fixes to HB references and added “third party” to 3c.</p>

Table of Contents

Contents

1	INTRODUCTION	1
1.1	Background	1
1.2	Purpose of the CMVP Management Manual	1
1.3	Purpose of the CMVP	1
1.4	Purpose of the Cryptographic Algorithm Validation Program (CAVP)	2
1.5	Use of Validated Products	2
1.6	CMVP Management Manual Structure	2
1.7	CMVP Related Documents	3
1.7.1	FIPS 140-3	3
1.7.2	Security Requirements for Cryptographic Modules	3
1.7.3	Test requirements for cryptographic modules	4
1.7.4	NIST SP 800-140x	4
1.7.5	Implementation Guidance and Request For Guidance	5
1.7.6	Web Cryptik User Guide	5
1.7.7	CSTL Accreditation Standards	6
1.7.8	Page Links on the CMVP Website Main Page	6
2	CMVP MANAGEMENT	9
2.1	Introduction	9
2.2	Validation Authority	9
2.3	Programmatic Directives, Policies, Internal Guidance and Documentation	9
2.4	CMVP Points of Contact	9
2.4.1	Language of Correspondence	10
2.5	Request for Guidance from CMVP	10
2.5.1	Request for Guidance Details	11
2.5.2	Request for Guidance Format	12
2.5.3	Post Validation Inquiries	12
2.6	Roles and Responsibilities of Program Participants	13
2.6.1	Vendor	13
2.6.2	Cryptographic and Security Testing Laboratory	13
2.6.3	CMVP Validation Authorities	15
2.6.4	Validated Module User	15
2.7	CMVP Meetings	15
2.7.1	CSTL Manager Meetings	16

2.7.2	CMUF participation	16
2.8	Confidentiality of Information	17
3	CSTL PROCESSES	18
3.1	Accreditation of CMVP scopes for CSTLs	18
3.1.1	Accreditation Process for the CMVP scope	18
3.2	Maintenance of CSTL Accreditation	22
3.2.1	Proficiency of CSTL	22
3.2.2	Renewal of Accreditation	23
3.2.3	Ownership of a CSTL	23
3.2.4	Relocation of a CSTL	23
3.2.5	Change of Approved Signatories	23
3.2.6	Change of Key Laboratory Testing Staff	24
3.2.7	Monitoring Visits	24
3.2.8	Extended Cost Recovery	24
3.2.9	Suspension of Accreditation	26
3.2.10	Revocation of Scope	26
3.3	Confidentiality of Proprietary Information	26
3.3.1	Confidentiality of Proprietary Information Exchanged between NIST, CCCS and the CSTL	26
3.3.2	Non-Disclosure Agreement for Current and Former Employees	27
3.4	Code of Ethics for the CSTLs	27
3.5	Management of CMVP and CAVP Test Tools	27
4	CMVP PROCESSES	28
4.1	Cryptographic Module Validation Process Overview	28
4.1.1	Vendor, CSTL, and CMVP duties for Testing of the Cryptographic Module	28
4.2	Implementation Under Test (IUT) and Modules in Process (MIP)	31
4.3	Validation Submission Queue Processing	31
4.3.1	Full and Update Submission Validations	31
4.3.2	All other submissions	31
4.3.3	Request for Transition Period Extension	32
4.3.4	HOLD Status for Cryptographic Modules on the Modules In Process	32
4.3.5	Resubmission while in Review Pending	33
4.3.6	Changes while in Coordination	33
4.3.7	Validation Deadline	34
4.4	Validation when Test Reports are not Reviewed by both Validation Authorities	34
4.4.1	Controlled Unclassified Information	34
4.5	CMVP Fees	36
4.5.1	Cost Recovery Program (CR & ECR)	36
4.5.2	NIST Payment Policy	36
4.5.3	Invoice for a Report Submission	36
4.6	Flaw Discovery Handling Process	37

4.7	Historical or Revoked Validations	37
4.8	Entropy Source Validation (ESV) Processes	38
4.8.1.1	Entropy Source Validation Submissions	39
4.8.1.2	Entropy Source Validation Web Client	40
4.8.1.3	Entropy Source Validation Python Client	40
4.8.2	Entropy Source Validation Comment Remediation Process	41
4.8.3	Entropy Source Validation Webpages	41
4.9	CMVP Webpages	41
4.9.1	Official CMVP Website	41
4.9.2	Cryptographic Module Validation Lists	41
4.9.3	CMVP Certificate Page Links	43
4.9.3.1	Security Policy	43
4.9.3.2	Consolidated Validation Certificate	43
4.9.3.3	Vendor Link	43
4.9.3.4	Vendor Product Link	43
4.9.3.5	Algorithm Certificates	43
4.9.3.6	Validation History	44
4.9.4	Usage of FIPS 140-3 Logos	44
5	CMVP AND CAVP PROGRAMMATIC METRICS COLLECTION	45
5.1	Overview	45
5.2	Confidentiality of the Collected Metrics Data	45
5.3	Collected Metrics	45
6	TEST TOOLS	46
6.1	Web Cryptik	46
6.2	Suggested Tools for Physical Testing	46
7	CMVP GENERAL TESTING AND REPORTING GUIDANCE	48
7.1	Submission Scenarios	48
7.1.1	Requirements for all revalidations	48
7.1.2	Full Submission (FS)	49
7.1.2.1	Interim Validation	50
7.1.3	Vendor Update (VUP)	50
7.1.4	Vendor Affirmed Operational Environment (VAOE)	50
7.1.5	Non-Security Relevant (NSRL)	50
7.1.6	Algorithm Update (ALG)	52
7.1.7	Operational Environment Update (OEUP)	52
7.1.8	Rebrand (RBND)	53
7.1.9	Port Sub Chip (PTSC)	54
7.1.10	Update (UPDT)	55
7.1.11	Common Vulnerabilities and Exposures (CVE)	56
7.1.12	Algorithm Transition (TRNS)	57
7.1.13	Physical Enclosure (PHYS)	61
7.1.14	Submission Scenario Summary Table	62
7.1.15	Additional Comments	63

7.2 CMVP requirements pertaining to testing and approved algorithms	65
7.2.1 Vendor Affirmation of Security Functions and Methods	65
7.2.2 Transitioning from vendor affirmed to CAVP Testing	66
7.3 Testing using Emulators and Simulators	67
7.4 Remote Testing of Modules	68
7.5 Partial validations and non-applicable areas	71
7.6 CMVP requirements for PIV validations	71
7.7 Module count definition	72
7.8 Module definitions for same certificates	72
7.9 Vendor or User Affirmation of Modules	72
7.9.1 Vendor	73
7.9.2 User	74
7.10 Operational Equivalency Testing for HW Modules	75
ANNEX A CMVP POST VALIDATION ISSUE ASSESSMENT PROCESS	78
Annex A.1 Addressing Security Relevant Issues	78
Annex A.2 Addressing CVE Relevant Vulnerabilities	79

ACRONYMS 80

List of Figures

Figure 1 - Roles, Responsibilities, and Output in the CMVP Process.....	13
Figure 2 - CSTL NVLAP scopes	18
Figure 3 - CSTL Accreditation Process	19
Figure 4- Cryptographic Module Testing and Validation Process	28
Figure 5- Annex A. Validation Issue Assessment Process	78

List of Tables

Table 1 - CAVP testing release dates and subsequent CMVP Transition dates.....	66
Table 2 - Equivalence Categories	75

1 Introduction

2 1.1 Background

3 The Canadian Centre for Cyber Security (CCCS) and the National Institute of Standards and
4 Technology (NIST) announced the establishment of the Cryptographic Module Validation
5 Program (CMVP) on July 17, 1995. The CMVP validates commercial cryptographic modules to
6 Federal Information Processing Standard (FIPS) 140, NIST-recommended standards, and other
7 cryptography-based standards. The CMVP is a government validation program that is jointly
8 managed by NIST and CCCS. Cryptographic modules validated as conforming to FIPS 140 are
9 used by Federal agencies for the protection of Controlled Unclassified Information (CUI)
10 (Government of the United States of America) or Protected information (Government of
11 Canada).

12 Vendors of commercial cryptographic modules use independent, National Voluntary Laboratory
13 Accreditation Program (NVLAP) accredited Cryptographic and Security Testing (CST)
14 laboratories to have their modules tested. The Cryptographic and Security Testing Laboratories
15 (CSTL)s may perform all of the tests covered by the CMVP. The Validation Authority reviews
16 laboratory reports, issues validation certificates, and participates in laboratory accreditations.

17 1.2 Purpose of the CMVP Management Manual

18 The purpose of the CMVP Management Manual is to provide effective management guidance
19 for the CMVP, CST labs, and the vendors who participate in the program. Consumers who
20 procure validated cryptographic modules may also be interested in the contents of this manual.

21 This manual outlines the management activities, processes, and responsibilities that have been
22 assigned to the various participating groups. This manual includes administrative guidance. For
23 technical aspects of the requirements of the referenced standards, please refer to the [CMVP](#)
24 [webpage](#) and associated links (e.g., FIPS 140-3 IG and RFG Announcements).

25 1.3 Purpose of the CMVP

26 The purpose of the CMVP is to increase assurance of secure cryptographic modules through an
27 established process.

28 Prior to CMVP, each office was responsible for assessing encryption products with no
29 standardized requirements. This meant that each office needed some expertise in evaluating
30 manufacturing practices for cryptographic equipment and vendors would have to support each
31 office in their evaluation. With the establishment of the CMVP, a standards-based assessment
32 could be uniformly applied and used across the federal governments and other organizations
33 finding value in the use of validated cryptography.

34 CMVP validation is performed through conformance testing to requirements for cryptographic
35 modules as specified in FIPS 140. Accredited third-party CSTLs perform independent assurance
36 testing with CMVP oversight. CMVP is the Validation Authority, a joint initiative between the
37 Government of Canada and the Government of the United States of America. For more

38 information about CMVP see: [https://csrc.nist.gov/projects/cryptographic-module-validation-](https://csrc.nist.gov/projects/cryptographic-module-validation-program)
39 [program](https://csrc.nist.gov/projects/cryptographic-module-validation-program).

40 **1.4 Purpose of the Cryptographic Algorithm Validation Program (CAVP)**

41 The purpose of the CAVP is to increase assurance of cryptographic algorithms through a testing
42 process. Validation is achieved by testing the algorithm and comparing results to known or
43 expected answers. Tests are to demonstrate compliance with cryptographic standards listed in SP
44 800-140C, SP 800-140D, and SP 800-140E. More information about CAVP can be found at:
45 <https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program>.

46 **1.5 Use of Validated Products**

47 FIPS 140 requirements are applicable to all U.S. Federal agencies, but private sectors can use
48 cryptographic modules validated to FIPS 140 for the protection of sensitive information. Federal
49 agencies must use cryptographic-based security systems to provide adequate information security
50 for all operations and assets as defined in 15 U.S.C. § 278g-3. Additionally, cryptographic
51 modules must meet the requirements outlined in the FIPS 140 standards in order to comply with
52 the [FISMA](#) mandate.

53 Non-validated cryptography is viewed as providing no protection to the information or data—in
54 effect the data would be considered unprotected plaintext. If the agency specifies that the
55 information or data be cryptographically protected, then FIPS 140 is applicable. In essence, if
56 cryptography is required, then it must be validated.

57 Similarly, the CCCS *recommends* that GC departments and agencies use those validated
58 cryptographic modules for the protection of Protected information.

59 **1.6 CMVP Management Manual Structure**

60 This manual is organized into the following sections:

61 **Section 1 – Introduction** provides an introduction and overview of the CMVP.

62 **Section 2 – CMVP Management** describes the management of the CMVP
63 including the organization, administration, roles and responsibilities, and policies.

64 **Section 3 – CSTL Processes** describes the CSTL processes including accreditation,
65 maintenance, and management of a laboratory.

66 **Section 4 – CMVP Processes** describes the various aspects of the cryptographic
67 module validation process.

68 **Section 5 – CMVP and CAVP Programmatic Metrics Collection.**

69 **Section 6 – Test Tools** describes the necessary and recommended tools for use by the
70 CSTLs.

71 **Section 7 – CMVP General Testing and Reporting Guidance** adds requirements to
72 manage the CMVP testing program, minimizing retest and maximizing testing

73 flexibility while maintaining assurance.

74 **Annex A –Validation Issue Assessment Process** provides an overview how
75 contentious issues over module previously validated are addressed.

76 **1.7 CMVP Related Documents**

77 FIPS 140 specifies the security requirements for a cryptographic module utilized within a
78 security system protecting sensitive information in computer and telecommunication systems.
79 The CMVP utilizes a set of documents, identified below, containing the security requirements
80 and testing of those requirements that must be satisfied by a cryptographic module. CMVP also
81 works with NVLAP to address CSTL accreditation requirements. A diagram of the relationships
82 for the documents referenced below is available on the CMVP webpage (www.nist.gov/cmvp)
83 under *CMVP FIPS 140-3 Related References*.

84 1.7.1 FIPS 140-3

85 Federal Information Processing Standards FIPS 140-3 identifies the CMVP, a joint effort of the
86 US and Canadian governments, as the validation authority for implementing a program utilizing
87 the ISO/IEC 19790:2012 requirements standard and ISO/IEC 24759:2017 derived test methods.
88 The standard also established the CMVP technical requirements to be contained in NIST Special
89 Publication (SP) 800-140, SP 800-140A, SP 800-140B, SP 800-140C, SP 800-140D, SP 800-
90 140E, and SP 800-140F, and their latest revisions. These security requirements must be satisfied
91 by a cryptographic module utilized within a security system protecting controlled unclassified
92 information (hereafter referred to as sensitive information). This standard supersedes FIPS 140-
93 2, Security Requirements for Cryptographic Modules, in its entirety. FIPS 140-3 is available on-
94 line at <https://doi.org/10.6028/NIST.FIPS.140-3>.

95 **Responsible Positions:** NIST CMVP and CCCS CMVP Program Managers.

96 1.7.2 Security Requirements for Cryptographic Modules

97 ISO/IEC 19790:2012 (with Technical Corrigendum 1 in 2015) specifies the security
98 requirements for a cryptographic module utilized within a security system protecting sensitive
99 information in computer and telecommunication systems. This International Organization for
100 Standardization, (ISO) standard defines different levels for cryptographic modules to provide for
101 a wide spectrum of data sensitivity (e.g., low value administrative data, million-dollar funds
102 transfers, life protecting data, personal identity information, and sensitive information used by
103 government) and a diversity of application environments (e.g., a guarded facility, an office,
104 removable media, and a completely unprotected location). The ISO/IEC Standard specifies four
105 security levels with 11 requirement areas, each security level increasing security requirements
106 over the preceding level.

107 The standard is typically reviewed by an ISO committee every three years for consideration of
108 revision. Copies can be obtained from ISO.org. NIST made available a limited number of copies
109 of ISO/IEC 19790:2012. To request a copy of ISO/IEC 19790:2012 and ISO/IEC 24759:2017
110 (see below), see the CMVP webpage, <https://csrc.nist.gov/Projects/cryptographic-module->

111 [validation-program/fips-140-3-standards](#).

112 **Responsible Positions:** ISO technical committee: [ISO/IEC JTC 1/SC 27](#) Information
113 security, cybersecurity and privacy protection.

114 1.7.3 Test requirements for cryptographic modules

115 ISO/IEC 24759:2017 specifies the methods to be used by accredited CSTLs to test whether the
116 cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012. The test
117 requirements (TR) contains the security requirements from ISO/IEC 19790:2012, stated as a set
118 of assertions (AS) (i.e., statements that must be true for the cryptographic module to satisfy the
119 requirement of a given area at a given level). All assertions are direct quotations from ISO/IEC
120 19790:2012. Following each assertion is a set of information requirements that must be fulfilled
121 by the vendor as vendor evidence (VE). These VEs describe the types of documentation or
122 explicit information that the vendor must provide in order for the tester to determine
123 conformance to the given assertion. Following each assertion and corresponding vendor
124 information requirement is a set of test evidence (TE) that must be applied by the tester of the
125 cryptographic module. These TEs instruct the tester as to what they must do in order to test the
126 cryptographic module with respect to the given assertion. ISO/IEC 24759:2017 VE and TE
127 requirements may be modified by the SP 800-140 set of documents and the FIPS 140-3
128 Implementation Guidance (IG).

129 **Responsible Positions:** ISO technical committee: [ISO/IEC JTC 1/SC 27](#) Information
130 security, cybersecurity and privacy protection.

131 1.7.4 NIST SP 800-140x

132 The current version of the following SPs can be found at:
133 <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards#sp> .
134 Each SP 800-140x document will be updated as needed, following the publication of a draft for
135 public comment and resolution by the CMVP.

136 **NIST SP 800-140** specifies the Test Requirements (TR) for Federal Information Processing
137 Standard (FIPS) 140-3. SP 800-140 modifies the TE and/or VE requirements of ISO/IEC
138 24759:2017. As a validation authority, the CMVP may modify, add, or delete TEs and/or VEs as
139 specified under section 5.2 of ISO/IEC 24759:2017. This NIST SP should be used in conjunction
140 with ISO/IEC 24759:2017 as it modifies only those requirements identified in this document.

141 **NIST SP 800-140A** modifies the vendor documentation requirements of ISO/IEC 19790:2012
142 Annex A. As a validation authority, the CMVP may modify, add, or delete VEs and/or TEs as
143 specified under section 5.2 of ISO/IEC 19790:2012. This document should be used in
144 conjunction with ISO/IEC 19790:2012 Annex A and ISO/IEC 24759:2017 paragraph 6.13 as it
145 modifies only those requirements identified in this document.

146 **NIST SP 800-140Br1** is to be used in conjunction with ISO/IEC 19790:2012 Annex B and
147 ISO/IEC 24759:2017 6.14. The SP modifies only those requirements identified in this document.
148 SP 800-140B also specifies the content of the tabular and graphical information required in
149 ISO/IEC 19790:2012 Annex B. As a validation authority, the CMVP may modify, add, or delete
150 VE and/or TE specified under paragraph 6.14 of ISO/IEC 24759:2017 and as specified in

151 ISO/IEC 19790:2012 paragraph B.1.

152 **NIST SP 800-140Cr2** replaces the approved security functions of ISO/IEC 19790:2012 Annex
153 C. As a validation authority, the CMVP may supersede this Annex in its entirety. This document
154 supersedes ISO/IEC 19790:2012 Annex C and ISO/IEC 24759:2017 paragraph 6.15.

155 **NIST SP 800-140Dr2** replaces the approved sensitive parameter generation and establishment
156 methods requirements of ISO/IEC 19790:2012 Annex D. As a validation authority, the CMVP
157 may supersede this Annex in its entirety. This document supersedes ISO/IEC 19790:2012 Annex
158 D and ISO/IEC 24759:2017 paragraph 6.16.

159 **NIST SP 800-140E** replaces the approved authentication mechanism requirements of ISO/IEC
160 19790:2012 Annex E. As a validation authority, the CMVP may supersede this Annex in its
161 entirety with its own list of approved authentication mechanisms. This document supersedes
162 ISO/IEC 19790:2012 Annex E and ISO/IEC 24759:2017 paragraph 6.17.

163 **NIST SP 800-140F** replaces the approved non-invasive attack mitigation test metric
164 requirements of ISO/IEC 19790:2012 Annex F. As a validation authority, the CMVP may
165 supersede this Annex in its entirety. This document supersedes ISO/IEC 19790:2012 Annex F
166 and ISO/IEC 24759:2017 paragraph 6.18.

167 **Responsible Positions:** NIST CMVP and CCCS CMVP Program Managers.

168 1.7.5 Implementation Guidance and Request For Guidance

169 *Implementation Guidance (IG) and Request For Guidance (RFG)* is issued to provide
170 clarification and guidance with respect to an assertion or group of assertions and requirements
171 found in the documents listed above. Often, this guidance is issued to assist CSTLs and vendors
172 to apply the requirements to a particular type of cryptographic module implementation or
173 technology. This guidance is also issued based on responses by NIST and CCCS to questions
174 posed by the CSTLs, vendors, and other interested parties. The IG and RFG posts are available
175 on-line on the official website at [https://csrc.nist.gov/Projects/cryptographic-module-validation-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements)
176 [program/fips-140-3-ig-announcements](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements).

177 **Responsible Position:** NIST CMVP and CCCS CMVP Program Managers.

178 1.7.6 Web Cryptik User Guide

179 This guide is available in the Help area of the Web Cryptik tool. It covers the use of FIPS 140-3
180 Web Cryptik. It is expected to be updated often as new functionality, edits, and program changes
181 are introduced. The user guide may also identify where IG information requested should be
182 included in the report and security policy. This guide also provides guidance on how to fill in
183 some of the available fields (e.g., laboratory information, vendor information). The guides for
184 various versions are also available at [https://csrc.nist.gov/Projects/cryptographic-module-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-series-supplemental-information/sp800-140b)
185 [validation-program/sp-800-140-series-supplemental-information/sp800-140b](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-series-supplemental-information/sp800-140b), in the Process
186 Support Applications section of the Module Package Creation tab.

187 **Responsible Position:** NIST CMVP and CCCS CMVP Program Managers.

188 1.7.7 CSTL Accreditation Standards

189 NIST laboratory accreditation standards applicable to the NVLAP accreditation of CSTLs are
 190 published on the NVLAP website at <https://www.nist.gov/nvlap>.

191 NIST laboratory accreditation standards relevant to the NVLAP accreditation of CSTLs are:

192 NIST Handbook 150 (2020), *NVLAP Procedures and General Requirements*,

193 NIST Handbook 150-17 (2022), *NVLAP Cryptographic and Security Testing*,
 194 Document

195 Links for these documents and associated Lab Bulletins are available at

196 <https://www.nist.gov/nvlap/publications-and-forms/nvlap-handbooks-and-lab-bulletins>.

197 **Responsible Position:** Chief of NVLAP.

198 1.7.8 Page Links on the CMVP Website Main Page

199 The CMVP website contain several FIPS 140-3 pages pertinent to the program:

- 200 1. [FAQs \(https://csrc.nist.gov/Projects/cryptographic-module-validation-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/faqs)
 201 [program/faqs\)](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/faqs) contains frequently asked questions and answers.
- 202 2. [Publications \(https://csrc.nist.gov/Projects/cryptographic-module-validation-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/publications)
 203 [program/publications\)](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/publications) contains the CMVP publications.
- 204 3. [Validated Modules \(https://csrc.nist.gov/Projects/Cryptographic-Module-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules)
 205 [Validation-Program/Validated-Modules\)](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules) contains a link to the search tool for finding
 206 a specific module or aspects of module validation. In addition, the page contains
 207 information describing categories (active, historical, and revoked) and explains the
 208 difference between a module that is a product and one that is a component. The
 209 [Caveats sub-page](#) describes the module validation caveats that may warn a user of
 210 specific stipulations, conditions, or limitations of a module, to assist in making a risk
 211 determination on its usage
- 212 4. [Modules in Process \(MIP\) List \(https://csrc.nist.gov/Projects/Cryptographic-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/Modules-In-Process-List)
 213 [Module-Validation-Program/Modules-In-Process/Modules-In-Process-List\)](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/Modules-In-Process-List) lists the
 214 review status for each cryptographic module whose scenario type is FS (Full
 215 submission) or UPDT (Update). The list tracks the test report after it has been
 216 submitted to the CMVP through validation. For each submission, the status and the
 217 date it went into that state is listed. The date will also be updated for any new
 218 submission to the CMVP, even if the status remains the same. For additional
 219 information regarding a specific module, please contact the vendor.
- 220 5. [Implementation Under Test \(IUT\) List](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List)
 221 [\(https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List)
 222 [In-Process/IUT-List\)](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List) contains information provided by the CSTLs about
 223 cryptographic modules undergoing testing. The result of the testing has not yet been
 224 submitted to the CMVP. Inclusion of a module on this list is voluntary, dependent on
 225 the vendor. The CMVP has no information regarding the status of these modules and
 226 does not know if or when a test report will be submitted to the CMVP. The modules

227 are listed by vendor name. For more information regarding a specific module, please
228 contact the vendor.

229 6. Entropy Validations

230 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-
232 validations](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-
231 validations)) This has a search page, announcements, and documents pertaining to the
Entropy Validations.

233 7. Programmatic Transitions ([https://csrc.nist.gov/Projects/cryptographic-module-
235 validation-program/programmatic-transitions](https://csrc.nist.gov/Projects/cryptographic-module-
234 validation-program/programmatic-transitions)) lists algorithm-related transitions.
236 Applicable standards, relevant IGs, ACVTS availability, and the beginning CMVP
237 acceptance date are listed for each algorithm/scheme. Also available is information
238 related to deprecated algorithms/schemes and whether they force validated module
239 certificates to the historical category. Included in this list are deadlines for last
240 submission date as an approved algorithm/scheme as well as the date whereby the
241 validation certificate of an approved module using the algorithm/scheme will be
moved to the Historical list.

242 8. CMVP FIPS 140-3 Management Manual
243 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-
140-3-management-manual](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-
244 140-3-management-manual)) contains the link to the latest version of this manual.

245 9. CMVP FIPS 140-3 Related References
246 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-
248 standards](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-
247 standards)) describes the FIPS 140-3 standard, referenced standards in FIPS 140-3,
and CMVP management documents.

249 10. FIPS 140-3 IG and RFG Announcements
250 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-
252 ig-announcements](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-
251 ig-announcements)) is where the latest version of the FIPS 140-3 IGs and RFGs can be
found. The webpage also includes a short summary of IG changes.

253 11. SP 800-140 Series Supplemental Information
254 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-
256 series-supplemental-information](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-
255 series-supplemental-information)) contains a table summarizing the SP 800-140x
257 series publications and their relationships to ISO/IEC 19790:2012(E) and ISO/IEC
258 24759:2017(E). The sub-pages of this webpage provide the supplemental information
associated with that SP 800-140x document.

259 12. FIPS 140-3 Resources ([https://csrc.nist.gov/Projects/cryptographic-module-
261 validation-program/140-3-resources](https://csrc.nist.gov/Projects/cryptographic-module-
260 validation-program/140-3-resources)) provides guidance referenced in the FIPS 140-3
262 Management Manual. As an example, specifically detailed validation and re-
263 validation information such as minimum testing requirements for revalidation and
equivalency can be found here. TE Documentation Guidance is also available.

264 13. Use of FIPS 140-3 or FIPS 140-2 Logo and Phrases

265 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/use-of-fips-
267 140-2-logo-and-phrases](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/use-of-fips-
266 140-2-logo-and-phrases)) References and information as to the proper use and
registration of CMVP FIPS 140 validation logos.

- 268 14. CVP Certification Exam Information
269 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-information)
270 [certification-exam-information](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-information)) In order to be a certified tester for a CSTL, an
271 individual must pass this exam.
- 272 15. NIST Cost Recovery Fees
273 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)
274 [recovery-fees](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)) NIST fees paid by CSTL for validations depending on scenario.
- 275 16. CSTL Accreditation and Fees ([https://csrc.nist.gov/Projects/Testing-](https://csrc.nist.gov/Projects/Testing-Laboratories)
276 [Laboratories](https://csrc.nist.gov/Projects/Testing-Laboratories)) contains a link to the name and location of every CSTL accredited to
277 perform Cryptographic and Security Testing. The list also includes a point of contact
278 for each CSTL.
- 279 17. CMVP Validation Process
280 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)
281 [recovery-fees](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)) Process flow showing the interactions between the CSTL, the Vendor,
282 and the CMVP throughout the validation process.
- 283 18. Archived Notices ([https://csrc.nist.gov/Projects/Cryptographic-Module-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Notices)
284 [Validation-Program/Notices](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Notices)) contains copies of statements published in the Federal
285 Register, programmatic or policy updates or information not related to CMVP
286 documents or test tools.
- 287 19. Validation Process Flow ([https://csrc.nist.gov/Projects/cryptographic-module-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-flow)
288 [validation-program/cmvp-flow](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-flow)) contains a diagram and description of the CMVP
289 validation process. This page also speaks to validations that have undergone patches
290 and CVEs and how that could impact the validation status, and the CMVP's
291 recommendation.

292 **Responsible Position:** NIST CMVP and CCCS CMVP Program Managers.

293 **2 CMVP Management**

294 **2.1 Introduction**

295 The purpose of this section is to describe the overarching management structure and principles of
 296 the CMVP.

297 **2.2 Validation Authority**

298 The validation authority is the CMVP. The CMVP is jointly managed by NIST and CCCS. NIST
 299 and CCCS have both signed agreements for the management of the program that contains
 300 precepts by which both parties must abide. Copies of the agreements are kept by the Partnerships
 301 Group at CCCS and by the Computer Security Division at NIST.

302 **2.3 Programmatic Directives, Policies, Internal Guidance and Documentation**

303 The CMVP issues programmatic directives, policies, internal guidance, and documentation to all
 304 CSTLs. These communications are normally distributed by email. These communications are
 305 very important and can seriously impact on-going validation efforts. Information will be
 306 incorporated into the CMVP documentation over time.

307 The CMVP will strive not to make those directives and guidance retroactive to previous
 308 validations. However, the status of previous validations may be affected. CSTLs are encouraged
 309 to provide timely comments to the CMVP about those communications.

310 **2.4 CMVP Points of Contact**

311 Questions concerning the general operation of the CMVP can be directed to either NIST or
 312 CCCS. If a vendor is under contract with a CSTL for cryptographic module or algorithm testing,
 313 the vendor must contact the contracted CSTL for all questions concerning the test requirements.

314 The email address cmvp@nist.gov will be used for the general public to contact NIST CMVP
 315 and will continue to be published on the website as the main CMVP email account for NIST. The
 316 cmvp@cyber.gc.ca email address will continue to be separately supported and used by the CCCS
 317 CMVP office.

318

319 For general correspondence:

General Information Email Address	Purpose and Use
cmvp@cyber.gc.ca	All correspondence and FIPS 140-2 submissions to the CCCS CMVP.
cmvp@nist.gov	General correspondence to the NIST CMVP.

sp800-140-comments@nist.gov	Comments on CMVP guidance using the CMVP comment template.
--	--

320

321 The NIST CMVP uses some additional emails for specific CSTL communications, per below.

322 Please only use the single email address required. PGP is used for encrypted email.

For CSTL use only	Purpose and Use
cmvplab@nist.gov	General correspondence to the NIST CMVP office that is not included below.
cmvpauto@nist.gov	For use in FIPS 140-2 module/report processing. For FIPS 140-3 submissions, no email address is used as Web Cryptik and Box have taken the place of this email.
cmvp-processing@nist.gov	For questions and errors related to processing module/report submissions.
cmvpitar@nist.gov	For use in FIPS 140-2 ITAR module/report processing. FIPS 140-3 ITAR communications will use this email address; however, for submissions, Box has taken the place of this email.

323

324 Note 1: In general, if you have been in direct email communication with a CMVP member then
325 continue to email them.

326 Note 2: CSTL correspondence to cmvplab@nist.gov and general correspondence to
327 cmvp@nist.gov should also be sent to cmvp@cyber.gc.ca unless the matter only relates to NIST
328 or CCCS.

329 Note 3: We also strongly recommend that the group/shared email addresses (cmvplab@nist.gov
330 and cmvp@cyber.gc.ca) not be put in the “CC” address line as a general rule to ensure that
331 someone in the appropriate CMVP area will read and respond to the mail. Our respective offices
332 will ensure that everyone who needs to be included will see the email.

333 The list of CMVP points of contact can also be found on the CMVP website at:
334 <https://csrc.nist.gov/projects/cryptographic-module-validation-program>.

335 **2.4.1 Language of Correspondence**

336 All correspondence between NIST, CCCS, NVLAP, and the CSTLs must be in the English
337 language only.

338 **2.5 Request for Guidance from CMVP**

339 The CMVP suggests reviewing the CMVP Management Manual, IGs, RFGs, the CMVP
340 Announcements, and CMVP Notices posted on the CMVP websites first as answers to questions

341 may be readily available. The information found on the CMVP website provides the official
342 position of the CMVP. If the information cannot be found in the aforementioned guidance,
343 CMVP will accept request for guidance (RFG) from the CMVP that are general knowledge or to
344 a specific application. In addition, CMVP will accept post-validation RFGs for any perceived
345 issues relating to existing modules.

346 **Vendors** who are under contract with a CSTL for cryptographic module or algorithm testing of a
347 specific implementation(s) must contact the contracted CSTL for any questions concerning the
348 test requirements and how they affect the testing of the implementation(s).

349 Once a vendor is under contract with a CSTL, CMVP will only provide official guidance and
350 clarification for the vendor's module through the point of contact at the CSTL. In a situation
351 where the vendor and CSTL are at an irresolvable impasse over a testing issue, the vendor may
352 submit an RFG directly to the CMVP. The point of contact at the CSTL must be included in the
353 distribution of this correspondence. All correspondence from CMVP to the vendor on the issue
354 will be issued through the CSTL point of contact.

355 All RFGs must be in the below Request for Guidance Format and be sent to both
356 cmvplab@nist.gov and cmvp@cyber.gc.ca. Do not send the requests to individuals.

357 **Federal agencies and departments, and vendors not under contract** with a CSTL who have
358 specific questions about cryptographic module testing requirements or any aspect of the CMVP
359 should contact the appropriate NIST and CCCS points of contact. Questions can either be
360 submitted by e-mail, telephone, or written (if electronic document, Microsoft Word document
361 format is preferred).

362 **CSTLs** may submit test-specific or more general RFGs. All RFGs must be in the below Request
363 for Guidance Format and be sent to both cmvplab@nist.gov and cmvp@cyber.gc.ca. Do not
364 send the requests to individuals.

365 2.5.1 Request for Guidance Details

366 Requests must be aimed at clarifying issues about cryptographic module testing or other aspects
367 of the CMVP and must be submitted to the CMVP written in the RFG format described below.

368 A response may require internal review by both NIST and CCCS, as well as with others as
369 necessary, and may require follow-up questions from the CMVP. Therefore, such requests, while
370 time-sensitive, may not be resolved immediately. If the CMVP has not sent feedback within a
371 month, a follow-up status request is recommended.

372 CMVP replies to RFGs will state current policy or interpretations with every attempt made to be
373 accurate, consistent, and clear, on a timely basis. However, these are non-binding and subject to
374 change once the full report submission is received.

375 To increase collaboration, transparency, and consistency, the CMVP strongly recommends
376 submitting RFGs that are NON-PROPRIETARY, so that the RFG and CMVP resolution can be
377 made public to benefit the community (see [FIPS 140-3 IG and RFG Announcements](#)). The
378 CMVP may leverage experts within the Cryptographic Module User Forum (CMUF) Working
379 Group to help with the RFG recommended response. The CMVP will remove identifiable
380 information if requested by the submitter.

381 The email will have the subject line “[ID]-FIPS140-3-RFG-[NAME]-yyMMdd-N” where ID is
 382 the two-digit CSTL code (if not applicable, enter NA), NAME is the submitters name (e.g.,
 383 CSTL, vendor), yyMMdd is the year, month, and day of submission, and N is the number of
 384 RFGs with the same subject line sent on the same day (so they are each unique).

385 Example 1: [NA-FIPS140-3-RFG-VendorA-230630-1](#)

386 Example 2: [99-FIPS140-3-RFG-CSTL_A-230630-1](#)

387 Example 3: [99-FIPS140-3-RFG-CSTL_A-230630-2](#)

388

389 If an International Traffic in Arms Regulations (ITAR) RFG submission, email
 390 cmvpitar@nist.gov **only** using PGP encryption, and indicate it is “ITAR” appended to “RFG”.
 391 E.g.: 99-FIPS140-3-RFG_ITAR-CSTL_A-230630-1.

392 2.5.2 Request for Guidance Format

393 For each RFG, the following template must be used in either Word or PDF (preferred) format:

394 [https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-](https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/RFG%20Template.docx)
 395 [program/documents/fips%20140-3/RFG%20Template.docx](https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/RFG%20Template.docx)

396 2.5.3 Post Validation Inquiries

397 Once a module is validated and posted on the NIST CMVP website, many parties review and
 398 scrutinize the merits of the validation. These parties may be potential procurers of the module,
 399 competitors, academics, or others. If a party performing a post-validation review believes that a
 400 conformance requirement has not been met and this was not determined during testing or
 401 subsequent validation review, the party may submit an inquiry to the CMVP for review.

402 An Official Request must be submitted to the CMVP in writing with a signature following the
 403 guidelines above. If the requestor represents an organization, the official request must be on the
 404 organization’s letterhead. The assertions must be objective and not subjective. The module must
 405 be identified by reference to the validation certificate number(s). The specific technical details
 406 must be identified and the relationship to the specific FIPS 140 Derived Test Requirements
 407 assertions must be identified. The request must be non-proprietary and not prevent further
 408 distribution by the CMVP.

409 The CMVP will distribute the unmodified official request to the CSTL that performed the
 410 conformance testing of the identified module. The CSTL may choose to include the participation
 411 of the vendor of the identified module during its determination of the merits of the inquiry. Once
 412 the CSTL has completed its review, it will provide to the CMVP a response with a rationale on
 413 the technical validity regarding the merits of the official request.

414 The CSTL will state its position on its review of the official request regarding the module:

- 415 1. is without merit and the validation of the module is unchanged.
- 416 2. has merit and the validation of the module is affected. The CSTL will further state its
 417 recommendations regarding the impact to the validation.

418 The CMVP will review the CSTL’s position and rationale supporting its conclusion. If the
 419 CMVP concurs that the official request is without merit, no further action is taken. If the CMVP

420 concurs that the official request has merit, a security risk assessment will be performed regarding
 421 the non-conformance issue. Please see [Annex A](#) for the flow diagram illustrating the assessment
 422 process.

423 **2.6 Roles and Responsibilities of Program Participants**

424 The various roles and responsibilities of the participants in the CMVP are illustrated in Figure 1
 425 below.

Who	Vendor	CSTL	CMVP	User
Function	Designs & Produces	Tests for Conformance	Reviews & Approves	Specifies & Purchases
Output	Cryptographic Modules	Assessment Report	Validation List	Security with Assurance

426 *Figure 1 - Roles, Responsibilities, and Output in the CMVP Process*

427 **2.6.1 Vendor**

428 The role of the vendor is to design and produce cryptographic modules that comply with the
 429 requirements specified in the applicable ISO/IEC standards and NIST SPs. Among other
 430 functions, the vendor defines the boundary of the cryptographic module, determines its modes of
 431 operation and its associated services, and develops an entropy and algorithm strategy and provide
 432 the information for the non-proprietary security policy. The security policy generation
 433 information can be found in <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-series-supplemental-information/sp800-140b>. When a cryptographic
 434 module is ready for testing, the vendor submits the module and the associated documentation to
 435 the accredited CSTL of its choice.
 436

437 After the cryptographic module has been validated, the vendor manages post module validation
 438 through either a new validation or a revalidation process submitted by a CSTL. Any change to
 439 the module that is not part of either a validation or revalidation will invalidate the module.

440 **2.6.2 Cryptographic and Security Testing Laboratory**

441 The role of the CSTL is to independently test the cryptographic module to the requirements
 442 defined for the FIPS 140-3 security level and embodiment, and to produce a written test report
 443 for the CMVP Validation Authorities based on its findings. The CSTL can conduct algorithmic
 444 testing and verify compliance with the algorithm standards (there may be additional requirements
 445 beyond what is CAVP-tested), review the cryptographic module’s documentation and source
 446 code, and perform the required testing of the module in accordance with the TR, SP 800-140x
 447 and IG. All testing is performed or witnessed by a CVP tester. If a cryptographic module
 448 conforms to all the requirements of the standards, the CSTL submits a written report to the
 449 Validation Authority (CMVP). If a cryptographic module does not meet one (or more)

450 requirements, the CSTL may work with the vendor to resolve all discrepancies prior to
451 submitting the validation package to the Validation Authority. The CSTL reports to the vendor
452 any implementations do not meet the FIPS 140-3 testing requirements. CSTLs can not submit
453 non-conformant modules to the CMVP for validation without penalties.

454 CSTLs must confirm that claimed approved algorithms and security functions are compliant with
455 all requirements of their respective standards (Special Publications) when some ‘shall’
456 statements are not addressed by CAVP testing. If such compliance is not clearly demonstrated in
457 the validation report, the CMVP may require the CSTL to fill in tables or answer related
458 questions prior to validation. It is the CSTL’s responsibility to ensure and demonstrate full
459 compliance for approved cryptographic claims of the module, including requirements not
460 covered by CAVP tests.

461 The following information is supplemental to the guidance provided by NVLAP, and further
462 defines the separation of the design, consulting, and testing roles of the laboratories. The CMVP
463 policy in this area is as follows:

- 464 1. A CSTL may not perform validation testing on a module for which the laboratory has:
 - 465 a. designed any part of the module,
 - 466 b. developed original documentation (e.g., design specifications) for any part of the
467 module,
 - 468 c. built, coded, or implemented any part of the module, or
 - 469 d. any ownership or vested interest in the module.
- 470 2. Provided that a CSTL has met the above requirements, the laboratory may perform
471 validation testing on modules produced by a company when:
 - 472 a. the laboratory has no ownership in the company,
 - 473 b. the laboratory has a completely separate management from the company, and
 - 474 c. business between the CSTL and the company is performed under contractual
475 agreements, as done with other clients.
- 476 3. A CSTL may provide clarification of the *Security requirements for cryptographic*
477 *modules*, the *Test requirements for cryptographic modules*, and other associated
478 documents at any time during the life cycle of the module.
- 479 4. A CSTL may also create the Finite State Model (FSM), Security Policy, Entropy
480 Assessment Report (EAR) for an Entropy Source Validation, entropy Public Use
481 Document (PUD), Non-administrator guidance, and Administrator guidance, which are
482 specified as vendor documentation in FIPS 140-3. These must be taken from existing
483 vendor documentation for an existing cryptographic module (post-design and post-
484 development) and consolidated or reformatted from the existing information (from
485 multiple sources) into a set format. CMVP must be notified of this at the time of
486 submission by providing the listing of the CSTL generated documents required in ISO
487 24759 TEB.01.01. The CSTL must be able to show a mapping from the consolidated or
488 reformatted CSTL-created documentation back the original vendor source documentation.
489 The mapping(s) must be maintained by the CSTL as part of the validation records. Source

490 code information is considered vendor-provided documentation and may be used in the
491 CSTL-created documentation.

492 2.6.3 CMVP Validation Authorities

493 The CMVP Validation Authority is a joint effort of the National Institute of Standards and
494 Technology for the Government of the United States of America and the Canadian Centre for
495 Cyber Security for the Government of Canada.

496 The role of the Validation Authorities is to establish a program to validate the testing for every
497 cryptographic module. The tests are performed, and results are documented in the submission
498 package prepared by a CSTL and reviewed by the CMVP. If the cryptographic module is
499 determined to be compliant, then the module is validated, a validation certificate is issued, and
500 the module validation list (available on-line) is updated. During the review process, the
501 Validation Authorities submit any questions they may have to the CSTL. The questions are
502 typically technical in nature and are intended to ensure that the cryptographic module meets the
503 requirements of the standard and that the information provided is accurate and complete. The
504 CSTL may need to re-submit the validation submission along with supporting documentation
505 such as a draft validation certificate, validation report, or security policy.

506 The CMVP participates, on behalf of NVLAP, in the CSTL accreditation process, which
507 includes reviewing the management system, creating and administering the proficiency exam,
508 performing the on-site assessment, and overseeing the artifact testing.

509 2.6.4 Validated Module User

510 The user verifies that a cryptographic module that they are considering procuring has been
511 validated and meets their requirements. A listing of validated cryptographic modules is
512 available from [https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-
513 Program/Validated-Modules/Search](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search). A non-proprietary security policy is posted on the list for
514 each validated cryptographic module so that a potential user can determine if the validated
515 cryptographic module provides cryptographic services and protection required for their
516 particular application and threat environment.

517 The CMVP validates specific versions of a cryptographic module, and the user must verify that
518 the version procured is, in fact, the validated version. The version numbers for a validated
519 cryptographic module are specified on the CMVP website and in the latest Security Policy.

520 Users can also develop product or system specifications that include the requirements for FIPS
521 140-3 validated cryptographic modules. It is important to note that a cryptographic module may
522 be a complete product or a component thereof. Therefore, understanding the boundary and
523 interface of the validated cryptographic module will help in the determination of an adequate
524 cryptographic product.

525 2.7 CMVP Meetings

526 The CMVP is jointly managed by NIST and CCCS. Decisions are made jointly by both
527 organizations, and the NIST and CCCS Program Managers communicate regularly. While most

528 CMVP internal meetings focus on interactions with the CSTL, the CSTL Manager Meeting is
529 focused on assessments and improvements of the CMVP program operations and management.

530 2.7.1 CSTL Manager Meetings

531 NIST and CCCS organize CSTL manager meetings (typically annually) to discuss issues relating
532 to the CMVP, CAVP, and CSTLs. An agenda is created and distributed to the CSTLs before the
533 meetings and presentation materials are distributed to the CSTLs for reference following the
534 meetings. CSTL managers are welcomed to add any new agenda items at any time. Typically,
535 the CSTL manager meetings are to minimally include the CSTL managers and the CMVP and
536 CAVP Validation Authorities, however CSTL staff may be invited to attend, space permitting. It
537 is mandatory for CSTLs to have at least one attendee at the CSTL manager meeting.

538 Usual discussion topics for CSTL manager meetings include the following:

- 539 ● Status of the CMVP
- 540 ● Changed or new CMVP processes and/or procedures
- 541 ● Standards updates
- 542 ● Laboratory accreditation process update news
- 543 ● Implementation Guidance in development
- 544 ● Status of the CAVP
- 545 ● Test tool development
- 546 ● Upcoming meetings and/or symposiums

547 When possible, CSTL manager meetings are collocated with the annual International
548 Cryptographic Module Conference (ICMC) so that CMVP and CSTLs can also directly interact
549 with the community at large.

550 2.7.2 CMUF participation

551 The Cryptographic Module User Forum (CMUF) (cmuf.org) was established in 2013 by module
552 vendors, users, and CSTLs to provide a platform for practitioners in the community of
553 UNCLASSIFIED Cryptographic Module (CM) and UNCLASSIFIED Cryptographic Algorithm
554 (CA) Validation Programs (VP). The CMUF formed the annual ICMC which was held along
555 with the CSTL manager meetings. CMVP participated in the Conference and found the ICMC to
556 be an excellent way to communicate with the community at large.

557 In recent years, CMUF has asked CMVP to attend and present at the scheduled (e.g., monthly)
558 meetings. In this way, CMVP has been able to communicate with both CSTLs and vendors to
559 define the planning and goals more clearly, while accepting feedback from the community. It has
560 also allowed CMVP to hear programmatic issues that vendors and CSTLs are experiencing or
561 anticipating in which CMVP may not have adequate awareness. CMUF also hosts working
562 groups composed of volunteers to address various topics related to the standards that need further
563 development.

564 **2.8 Confidentiality of Information**

565 The protection of vendor proprietary information is paramount to the success and credibility of
566 the CMVP and CAVP. Proper safeguards must be implemented by NIST, CCCS, and the CSTLs
567 to protect against unauthorized disclosure of vendors' proprietary information. Any potential or
568 actual breach of confidentiality could have an adverse effect on the NIST, CCCS, a CSTL's
569 accreditation, or the program.

570 As required by the CSTL accreditation standards listed in Section 3.1 of this manual, CSTLs are
571 required to establish and implement procedures for protecting the integrity and confidentiality of
572 data entry or collection, data storage, data transmission and data processing. CSTLs must protect
573 cryptographic module validation test reports, and any proprietary information when these
574 documents are submitted to NIST and/or CCCS outside of Web Cryptik / Box.

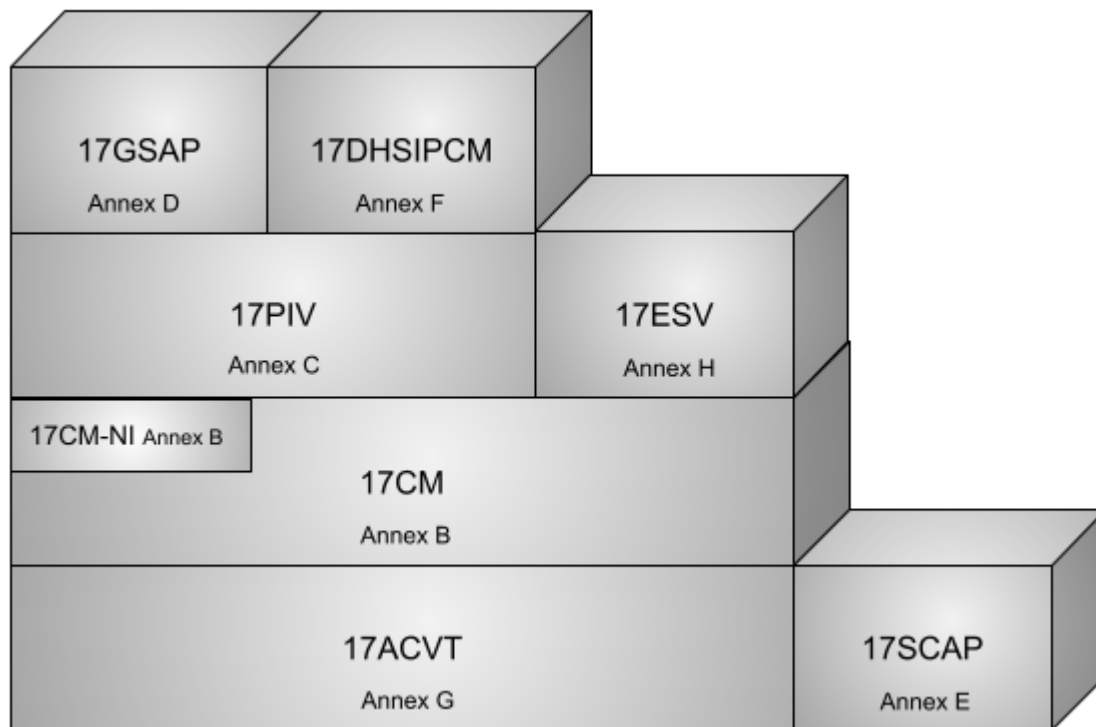
575 NIST, CCCS, and the CSTLs must ensure that personnel joining or departing these organizations
576 are advised of their responsibilities about safeguarding the vendor proprietary information they
577 may have been authorized to access during their period of employment.

578 **3 CSTL Processes**

579 This section describes administrative processes affecting CSTLs, including the granting and
 580 maintenance of accreditation, confidentiality of information, code of ethics, management of test
 581 data, and documentation.

582 **3.1 Accreditation of CMVP scopes for CSTLs**

583 This section describes in general terms the process for a laboratory to become an accredited
 584 CSTL for scope 17CM under the National Voluntary Laboratory Accreditation Program
 585 (NVLAP). Candidate laboratories may optionally apply for NVLAP 17CM-NI at the same time.
 586 17ESV is also supported by CMVP, though is considered a separate program. Laboratories are
 587 responsible for complying with the Cryptographic and Security Testing LAP which can be found
 588 at <https://www.nist.gov/nvlap/cryptographic-and-security-testing-lap>.



589
 590 *Figure 2 - CSTL NVLAP scopes*

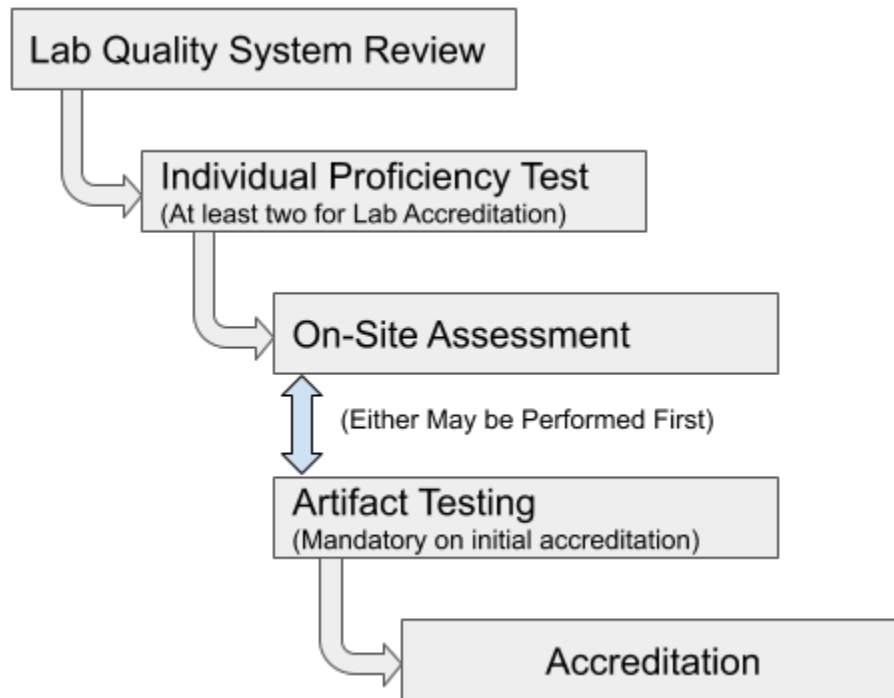
591 **NOTE:** Accreditation of the CAVP scope is necessary to obtain the 17CM scope for CMVP
 592 testing laboratories. For more information about CAVP accreditation, please see **Becoming a**
 593 **17ACVT Laboratory** on the CAVP website [https://csrc.nist.gov/Projects/cryptographic-](https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/how-to-access-acvts)
 594 [algorithm-validation-program/how-to-access-acvts](https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/how-to-access-acvts).

595 3.1.1 Accreditation Process for the CMVP scope

596 Applicant laboratories must complete the 17CM scope accreditation process within one year of

597 submitting the NVLAP application. Applications that are not completed within one year will
 598 have to be re-submitted, and the process will have to start again from the beginning. If the
 599 content of the accreditation process contained herein diverges from the aforementioned standards
 600 documents, those documents have precedence.

601 The accreditation process is illustrated in Figure 3. All steps in the accreditation process must be
 602 completed in the order shown.



603
 604 *Figure 3 - CSTL Accreditation Process*

605 3.1.1.1 Application for Accreditation and Selection of Assessment Team

606 The prospective CSTL must complete an application form, pay the respective fees, agree to the
 607 conditions of accreditation, and provide their quality system to NVLAP prior to the on-site
 608 assessment. Upon notification by NVLAP of an acceptable application, an assessment team is
 609 selected. This team is typically comprised of one or more technical assessors representing CMVP
 610 and one lead assessor from NVLAP. NVLAP technical assessors for CSTLs are selected by the
 611 NVLAP Program Manager and are chosen based upon their knowledge of the relevant FIPS
 612 standards and related documentation, NVLAP requirements, assessment techniques, and quality
 613 systems. The assessors must not have a conflict of interest with the CSTL they will be assessing.

614 3.1.1.2 Management System Evaluation

615 The assessment team will review the Management System to determine if it meets the
 616 requirements of NIST Handbook 150 and NIST Handbook 150-17.

617 3.1.1.3 CVP Proficiency Examination

618 Every independent tester, technical reviewer and submission signatory must maintain
 619 Cryptographic Validation Program (CVP) certification by passing the current proficiency exam.

620 The current written examination consists of approximately one hundred questions relating to
621 various aspects of CSTL activities, FIPS 140-3, and cryptographic algorithm implementation
622 testing. The exam is an individual certification exam. The certification exam will encompass the
623 domains listed below:

624 a. Physical Security

- 625 ○ Understand the different module types and different embodiments for
626 modules.
- 627 ○ Understand requirements for physical security for modules specific to levels 1-
628 4.

629 b. Authentication, Roles, Services, Software/Firmware Security and Operational
630 Environment

- 631 ○ Understand authentication requirements and concepts.
- 632 ○ Define the requirements for roles.
- 633 ○ Understand the concepts of services using approved and non-approved
634 functions, and the bypass capability.
- 635 ○ Understand the self-initiated cryptographic output capability,
636 Software/Firmware security including loading requirements and their
637 applicability.
- 638 ○ Describe the operational environment requirements/concepts and how to test
639 them.

640 c. Algorithms and Self-Tests

- 641 ○ Understand the concepts of the approved and allowed algorithms.
- 642 ○ Identify which algorithms are approved or allowed.
- 643 ○ Identify testing for components of the algorithms.
- 644 ○ Identify the tester's responsibilities when reviewing an algorithm's
645 implementation.
- 646 ○ Identify the pre-operational self-tests (e.g., integrity, bypass) and know the
647 associated requirements.
- 648 ○ Understand the requirements for conditional self-tests, including cryptographic
649 algorithm self-tests.

650 d. Sensitive Security Parameter (SSP) Establishment

- 651 ○ Understand the requirements for SSP generation, SSP agreement, SSP
652 transport and SSP derivation and applicable standards and guidance.
- 653 ○ Understand and identify the approved random bit generators.
- 654 ○ Understand the notion of entropy and methods of entropy estimation.
- 655 ○ Possess general knowledge of the SSP establishment protocols and standards
656 in the IT industry.

657 e. SSP Management

- 658 ○ Understand the requirements for SSP entry and output and trusted channels.
- 659 ○ Understand the requirements for SSP storage.
- 660 ○ Understand the various types of SSPs and their zeroization requirements.

661 f. Security Assurances

- 662 ○ Understand the requirements of module specification including degraded
663 operation, approved and non-approved modes.
- 664 ○ Understand the programmatic guidance and associated documentation
665 requirements.
- 666 ○ Understand the requirements for ports & interfaces, finite state model,
667 development, mitigation of non-invasive and other attacks, and design
668 assurance.

669 The exam is graded, and the results are recorded by the CMVP and provided to the exam taker.
670 CMVP provides an exam score if passed; otherwise, the scoring for each area not passed is
671 provided. Scoring is adjusted for the difficulty of the exam taken, but transparent to the exam
672 taker. An opportunity is provided for retaking the exam in the event of failure. Once passed, the
673 reexamination period for maintaining the certification for CVP certified testers is four years. In
674 the event of major program updates, e.g., a new FIPS 140 standard, the reexamination frequency
675 may be increased to encompass changes in the technical requirements. For the most up to date
676 information, refer to the CVP Certification Exam Information tab
677 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-information)
678 [information](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-information)) on the CMVP website.

679 3.1.1.4 On-Site Assessment

680 An on-site assessment of the laboratory is conducted to determine compliance with the
681 accreditation criteria. The on-site assessment is scheduled by the assessment team following
682 receipt of payment and a passing grade on the CST Proficiency Examination by a minimum of
683 two CST testers. An assessment typically takes two to three business days to perform. The
684 activities performed during an assessment are described in Section 3.3 of NIST Handbook 150.

685 For an **accredited** CSTL, any deficiencies found during the assessment, the laboratory must
686 submit a satisfactory plan concerning resolution of deficiencies to NVLAP within thirty days of
687 notification. If the plan for correcting deficiencies is not submitted within 30 days, the CSTL
688 may be suspended for the applicable scopes.

689 For an **applicant** CSTL, any deficiencies must be addressed by a satisfactory plan within thirty
690 days of notification and resolved before being eligible for accreditation.

691 3.1.1.5 Artifact Testing

692 After two testers pass the CVP exam or following the on-site assessment, the assessment team
693 may provide an artifact that the applicant laboratory must test and submit according to the
694 requirements and policies of the CMVP. The CMVP will then assess the competency of the
695 laboratory using the responses provided in the test report. The initial NVLAP application process
696 includes the testing of the artifact, all of which must be completed within one (1) year.

697 3.1.1.6 Accreditation Decision

698 The CMVP will make a recommendation of the applicant laboratory competency. NVLAP will
699 evaluate the results of the laboratory assessment and the CMVP recommendation, before making
700 the final accreditation decision.

701 3.1.1.7 Granting Accreditation

702 If approval has been granted to accredit the CSTL for Cryptographic Security testing, NVLAP
703 will assign the CSTL one of four renewal dates for the beginning of operation:

704 g. January 1

705 h. April 1

706 i. July 1

707 j. October 1

708 The accreditation period is one year. After initial accreditation, NVLAP will conduct an on-site
709 assessment after completing the first year of accreditation and then every two years thereafter
710 (see NIST HB 150, 3.2.3.3). The CSTL receives an NVLAP certificate and scope of
711 accreditation identifying the CSTL address, lab code, the CSTL's authorized representative, and
712 the expiration date of the accreditation.

713 3.1.1.8 CMVP Test Tools

714 Once accreditation has been granted and the CMVP is advised by NVLAP that the applicant
715 laboratory has been accredited, the CMVP will issue to the newly accredited CSTL access to the
716 latest version of Web Cryptik and associated tools. CMVP will also issue the latest
717 programmatic directives and policies, and internal guidance and documentation. The CSTL is
718 also required to have secure email capability using PGP for CUI communications unless
719 submitted through Web Cryptik. The lab is limited to two PGP email addresses in which to
720 communicate with the CMVP, of which one may be a shared email address within the CSTL.
721 PGP is not provided by the CMVP.

722 3.1.1.9 Cooperative Research and Development Agreement

723 All accredited CSTLs must execute a Cooperative Research and Development Agreement
724 (CRADA) agreement with NIST in order to do business with the CMVP. The agreement covers
725 the protection of information as well as the fees being charged by NIST for each type of CMVP
726 test report submission (scenario). This agreement is effective through October 31, 2026, with
727 amendments as required. New laboratories are required to execute the agreement once they
728 become accredited through NVLAP. Existing laboratories must re-execute the agreement upon
729 change or expiration. The NIST CMVP Program Manager is the point of contact for obtaining a
730 copy of the current CRADA.

731 **3.2 Maintenance of CSTL Accreditation**

732 3.2.1 Proficiency of CSTL

733 There is no requirement for a test report submission during the first year of accreditation. For all
734 successive years of accreditation, the following requirements apply. An accredited CST
735 laboratory must submit a minimum of two (2) test reports annually (every 12 calendar months) to

736 the validation authority to demonstrate continued testing proficiency.

737 This permits the CMVP staff to monitor the quality of the CSTL processes, the technical skills,
738 and knowledge of the CSTL staff. Failing this, NVLAP may suspend or revoke the CSTL's
739 accreditation.

740 In addition, laboratories are also required to have a minimum of two CVP FIPS 140 Certified
741 Testers throughout the accreditation period.

742 3.2.2 Renewal of Accreditation

743 Each accredited CSTL will receive a renewal application package before the expiration date of
744 its accreditation to complete the renewal process. Fees for renewal are charged in accordance
745 with the fee schedule published on the NVLAP website at [https://www.nist.gov/nvlap/nvlap-fee-
746 structure](https://www.nist.gov/nvlap/nvlap-fee-structure). Both the application and fees must be received by the accreditation body prior to the
747 expiration of the CSTL's current accreditation to avoid a lapse in accreditation.

748 The re-accreditation process is the same as illustrated in Figure 3 - CSTL Accreditation Process
749 and described in Section 3.1.1 above. If deficiencies are found during the assessment of an
750 accredited CSTL, the laboratory must submit to NVLAP a satisfactory plan outlining the
751 resolution of deficiencies within thirty days of notification. On-site assessments of accredited
752 laboratories are performed in accordance with the procedures in Section 3.3 of NIST Handbook
753 150.

754 3.2.3 Ownership of a CSTL

755 In the event a CSTL changes ownership, the accreditation body and the CMVP Validation
756 Authorities must be informed within ten (10) working days of the effective date of the change.
757 The CSTL must also submit an updated Quality System to NVLAP showing the new owner
758 information.

759 3.2.4 Relocation of a CSTL

760 In the event a CSTL relocates to a new facility, the laboratory director must submit a relocation
761 plan to the accreditation body and the CMVP at least one month before the relocation. The
762 relocation plan must demonstrate that the new location meets the requirements as set out in the
763 accreditation standards including information protection. The plan must also describe how
764 sensitive information will be moved between locations. The accreditation body and the CMVP
765 staff may conduct a monitoring visit after the relocation is completed to ensure all accreditation
766 requirements continue to be met. In addition, it should be noted that a change of location may
767 result in a change in customer ID for NIST billing.

768 3.2.5 Change of Approved Signatories

769 In the event of a change of the CSTL's Approved Signatories, the accreditation body and the
770 CMVP must be informed within thirty (30) working days of the new signatories and the effective
771 date of the change. All approved signatories must have passed the CVP exam prior to signing a
772 validation submission.

773 3.2.6 Change of Key Laboratory Testing Staff

774 Key personnel include:

- 775 a. laboratory director;
- 776 b. laboratory manager(s);
- 777 c. staff members(s) responsible for maintaining management system;
- 778 d. authorized representative;
- 779 e. approved signatories; and
- 780 f. other key technical persons in the laboratory (e.g., testers).

781 In the event of changes to key laboratory testing staff, the accreditation body and the CMVP
 782 must be informed of the new staff and the effective date of the change within thirty (30) working
 783 days. Failure to communicate laboratory staff changes to the accreditation body and the CMVP
 784 may result in an adverse action regarding accreditation. The laboratory must submit an updated
 785 organizational chart to NVLAP and the CMVP noting any changes.

786 3.2.7 Monitoring Visits

787 Monitoring visits may be conducted by the accreditation body at any time during the
 788 accreditation period, for cause or on a random basis. While most monitoring visits will be
 789 scheduled in advance with the CSTL, the accreditation body may conduct unannounced
 790 monitoring visits. The scope of the monitoring visits may range from an informal check of
 791 specific designated items to a complete review.

792 3.2.8 Extended Cost Recovery

793 Extended Cost Recovery (ECR) fees and points may apply when a submission results in one of
 794 the following categories:

795

Points	Category	Examples
0	Excessive CMVP time (non-errors)	<ol style="list-style-type: none"> 1. Excessive number of modules in one report. 2. Excessive submission size and/or complexity. 3. Special exception requests which require significant or specialized effort by CMVP. 4. Submitting RFGs on topics for which guidance has already been published, or not submitting an RFG in advance that results in significant effort to address during Coordination. 5. The module represents a new technology, a new type of fabrication, a unique implementation, or an unusual level of complexity and/or many functions and services.
1	Basic process errors	<ol style="list-style-type: none"> 1. Not following the CMVP submission process (e.g., not sending to the proper email address or account, TID duplication, improper use of encryption, missing required documentation,

		incomplete and/or inconsistent procedural/administrative documents).
2-3	Significant quality errors	<ol style="list-style-type: none"> 1. Submissions generate excessive comments or excessive non-productive comment rounds. 2. Incomplete technical documentation leaving open technical questions, due to missing, incomplete, or inconsistent technical claims. 3. Not addressing or following CMVP Implementation Guidance or other CMVP guidance. 4. Significant documentation issues that have a security impact (see section 4.7 'd' for examples). 5. Making unidentified changes to the module and/or documentation during Coordination or as part of a revalidation.
4	Severe submission process errors or process misuse	<ol style="list-style-type: none"> 1. Exposing or mishandling sensitive information such as bypassing protections. 2. A submission that is used as a placeholder, i.e., the report was not the intended version to be validated and/or was knowingly incorrect or incomplete.
5	Security non-conformance or inaccurate representation of a module	<ol style="list-style-type: none"> 1. Discovery of a security non-compliance or security flaw in a cryptographic module (typically one that would require module code changes to correct). 2. Purposely using incorrect information that misrepresents the module or its security features.

796
797
798
799
800
801
802
803
804
805
806

General ECR guidance:

1. Any of the above can apply to both module and ESV validations.
2. Depending on the issues identified, ECR may apply in cases where, post validation, a validated module is identified in the [Flaw Discovery Handling Process](#) and found to be incorrect.
3. Repeat ECR offenses may result in additional points (not to exceed 5 points) applied compared to what is listed in the table above.
4. The above ECR examples (non-exhaustive) may apply when clear CMVP guidance exists that was not followed.

807 An accredited laboratory must maintain an Extended Cost Recovery (ECR) point total of less
808 than 12 points. If a CSTL accumulates 12 or more points during the prior two (2) years, the
809 CMVP will recommend to NVLAP that the accreditation for the cryptographic module testing be
810 suspended.

811
812 If a CSTL has reached 6 or more points through the ECR process, the CMVP recommends the
813 following actions to pre-empt suspension:

814 The lab compiles a list of all reports in the Review Pending state in the CMVP
815 queue. Per policy, those reports are eligible for resubmission. If the CSTL elects to

816 review those submissions for potential resubmission, the CMVP may initiate up to a 30-
 817 day HOLD to allow the CSTL time to make any corrections needed prior to the reports
 818 moving to the In Review state. The CMVP would need to be notified in writing
 819 regarding which reports, if any, the CSTL would like to put on HOLD pending a
 820 resubmission. The final determination will be up to the CMVP.

821 3.2.9 Suspension of Accreditation

822 If NVLAP becomes aware that an accredited laboratory has violated the terms of accreditation,
 823 NVLAP may suspend the CSTL's accreditation. The determination by NVLAP whether to
 824 suspend the CSTL will depend on the nature of the violation(s). A letter from NVLAP will
 825 include a request for a remediation plan and an on-site review and artifact testing if needed.
 826 CSTLs must be in compliance with the NVLAP requirements prior to lifting the suspension.

827 Four areas of non-conformities that will lead to suspension of accreditation as stated in
 828 Handbook 150-17:

- 829 1. reports submitted for validation within the accreditation cycle are incorrect, invalid, or
 830 deficient as defined by each validation program (see [3.2.8](#));
- 831 2. the loss of key technical personnel from the CSTL;
- 832 3. nonconformities found during any onsite visit are not appropriately addressed through
 833 corrective actions taken by the CSTL; or
- 834 4. the CSTL has not submitted the required number of vendor product test reports to the
 835 validation authority within the accreditation cycle.

836 3.2.10 Revocation of Scope

837 If correcting the non-conformities is too onerous for the CSTL, the laboratory may elect to have
 838 NVLAP revoke the accreditation. A CSTL may at any time terminate its participation and
 839 responsibilities as an accredited laboratory by advising NVLAP and the CMVP in writing of its
 840 intent. Upon receipt of a request for termination, NVLAP must begin the termination process by
 841 notifying the CSTL that its accreditation has been terminated. The CSTL will be instructed to
 842 return its Certificate and Scope of Accreditation and to remove the accreditation body's logos
 843 from all test reports, correspondence, and advertising. Finally, the laboratory must return or
 844 provide signed confirmation of the destruction of all CMVP and CAVP provided material, test
 845 tools, and documentation. The CMVP will determine the course of action taken for any
 846 outstanding work that has not been completed. This will be handled on a case-by-case basis.

847 3.3 Confidentiality of Proprietary Information

848 Maintaining confidentiality of proprietary information is paramount to the operation of CMVP
 849 and requires the establishment and enforcement of appropriate controls.

850 3.3.1 Confidentiality of Proprietary Information Exchanged between NIST, CCCS and the CSTL

851 The confidentiality of the proprietary information exchanged between NIST, CCCS, and the
 852 CSTL is required by NVLAP at all times during and following the testing. All proprietary

853 materials must be marked as PROPRIETARY by the CSTL or the vendor.

854 3.3.2 Non-Disclosure Agreement for Current and Former Employees

855 The CSTL must develop and maintain non-disclosure agreements for staff that participate in the
856 testing of modules.

857 3.4 Code of Ethics for the CSTLs

858 The CSTL must:

- 859 1) Maintain NVLAP accreditation for the Cryptographic Security Testing Program;
- 860 2) Refrain from misrepresenting the scope of its accreditation;
- 861 3) Act legally and honestly;
- 862 4) Act ethically.

863 3.5 Management of CMVP and CAVP Test Tools

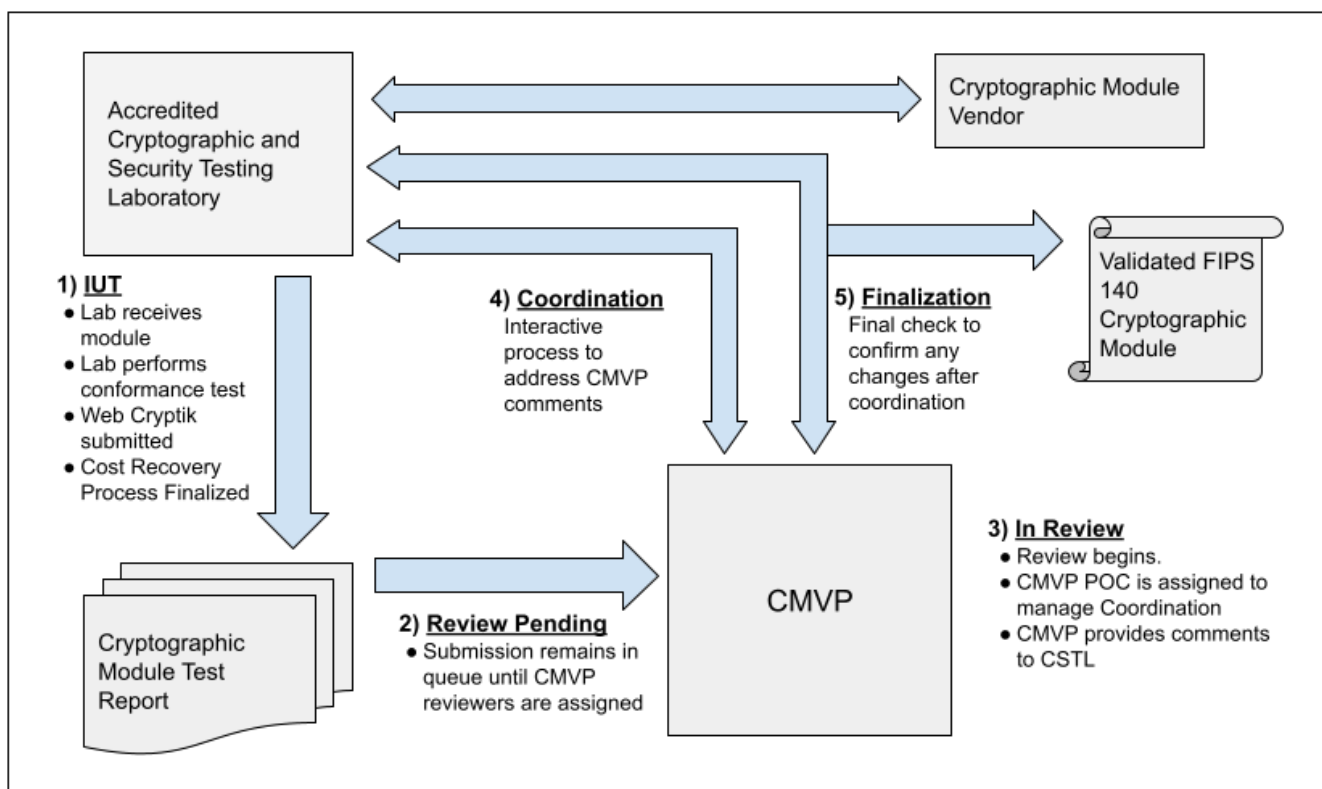
864 Test tools provided by NIST and CCCS must not be distributed to any entity outside the CSTL,
865 including firms contracted by the CSTL, unless explicitly authorized by CMVP management.
866 Personnel temporarily employed by and working under the supervision of a CSTL (i.e., a
867 contractor) can use the provided test tools when they are used within the CSTL facilities. Test
868 tools include all versions of Web Cryptik, the Automated Cryptographic Validation Testing
869 System (ACVTS), and any other tools provided by NIST and CCCS for use by the CMVP and
870 CAVP. Violation of this policy may be considered cause for suspension of the CSTL's
871 accreditation.

872 **4 CMVP Processes**

873 This section describes cryptographic module validation processes, including an overview of the
 874 program and the steps required to attain and maintain validation.

875 **4.1 Cryptographic Module Validation Process Overview**

876 This section provides a high-level overview of the validation program, primarily focused on the
 877 CSTL and CMVP interaction, followed by the vendor and laboratory interaction. The remaining
 878 subparagraphs work through the process performed by the vendor, CSTL, and CMVP for any
 879 submission, including full submissions and resubmissions. Figure 4 shows the general flow of
 880 testing and validation of a cryptographic module.



881
 882 *Figure 4- Cryptographic Module Testing and Validation Process*

883 **4.1.1 Vendor, CSTL, and CMVP duties for Testing of the Cryptographic Module**

884 A vendor contracts with an accredited CSTL to perform the cryptographic module validation
 885 testing. The vendor provides the CSTL with the necessary documentation and either provides the
 886 cryptographic module to the laboratory for testing or prepares it for testing at the vendor's
 887 facility.

888 To communicate specific validation information to CMVP, the CSTL must assign a Tracking
 889 Identification Number (TID). Once the laboratory is accredited, the CMVP assigns the first two
 890 digits of the TID; the second set of four digits is assigned by the CSTL and must be unique to the

891 validation. Validation-related submissions to CMVP should follow the instructions provided in
892 the Web Cryptik User Guide.

893 4.1.1.1 Implementation Under Test

894 Once vendor's contract has been executed and the vendor documentation is delivered to the
895 CSTL, the cryptographic module can begin testing. The CSTL may optionally notify CMVP that
896 the cryptographic module is to be included on the IUT List by providing the name of the
897 cryptographic module; the cryptographic module vendor's name. Inclusion in the IUT list is
898 voluntary. The module information on the IUT List will be removed after 18 months. The CSTL
899 will be notified when the IUT entry is dropped.

900 The CSTL performs the cryptographic module testing as prescribed by the ISO/IEC 24759:2017
901 *Test Requirements* (TR), the SP 800-140 series, and all applicable IGs. The testing information is
902 entered in the Web Cryptik tool. Although testing requirements are in the ISO/IEC 24759:2017
903 TR, ISO/IEC 19790:2012, *Security Requirements for Cryptographic Modules* remains the
904 definitive reference for whether or not the cryptographic module meets the requirements of the
905 standard. Any deviation from the *test requirements* that meet the *security requirements* needs to
906 be approved by CMVP prior to submission.

907 The cryptographic module validation process is an iterative process. At any point in the testing
908 the CSTL may wish to request guidance from CCCS and NIST in determining how to apply the
909 FIPS 140 standard to the particular cryptographic module. If the CSTL discovers any non-
910 conformances in the cryptographic module documentation or the cryptographic module itself, it
911 must bring details of the non-conformance(s) to the attention of the cryptographic module
912 vendor. The cryptographic module vendor must correct the non-conformance(s) and resubmit
913 updated documentation and the updated cryptographic module as necessary for validation
914 testing.

915 Once the CSTL completes all required cryptographic algorithm and entropy source validations
916 along with module testing, the CSTL can determine that the cryptographic module is conformant
917 to FIPS 140-3. The CSTL then prepares the submission using Web Cryptik. The CSTL
918 addresses each TE independently, not by referencing a response in another TE.

919 See the Web Cryptik User Guide for a summary table that describes what must be submitted by
920 the CSTL for validation. Web Cryptik aids the CSTL in preparing submissions, please refer to
921 the Web Cryptik User Guide and the [SP 800-140B Supplemental Information webpage](#) for
922 additional information.

923 4.1.1.2 Review pending

924 All FIPS 140 validation submissions received by the NIST and CCCS CMVP. If the initial
925 examination reveals issues, the CSTL is notified, and the submission is not accepted for review.
926 When the submission is accepted by the CMVP, the module is moved to the REVIEW
927 PENDING stage of the MIP List. Review pending transitions to In Review once the first
928 reviewer begins the review.

929 At the CMVP's discretion, a test report in this state may be subject to a triaged review to quickly
930 assess the quality of a report, and if needed, provide feedback to the lab. This triage activity is
931 implemented based on common issues observed from the submissions received by the CMVP.
932 Ability to quickly identify and address problematic submissions is paramount to not only

933 advance the FIPS 140-3 queue, but also be fair to all labs and vendors. Problematic submissions
934 will be sent back to the labs accompanied by generic statements for resolution. These reports *will*
935 maintain their respective queue positions.

936 **During periods when the CMVP submission queue is long, CSTLs are encouraged to**
937 **submit updated submissions to minimize any follow-on revalidations that might be**
938 **necessary (see [Section 4.4.5](#) *Resubmission while in Review Pending*).**

939 4.1.1.3 In Review

940 After the CMVP reviewers have been assigned to the submission, and the reviewer begins the
941 review, the cryptographic module is moved to the IN REVIEW stage of the MIP List. The
942 module validation must be completed and cannot exceed 24 months after transitioning to IN
943 REVIEW, or they will be subject to being dropped and would have to begin the process from the
944 start. Once they have completed their review of the validation submission and provided
945 comments, a comment file is sent to the CSTL. This event moves the cryptographic module to
946 the COORDINATION stage, described in Section 4.1.1.4.

947 4.1.1.4 Coordination

948 After receiving the comments from the CMVP and conferring with the vendor, as necessary, the
949 CSTL addresses the comments and resubmits a complete submission package containing any
950 modified documents. The reviewers examine the responses and respond with any additional
951 comments if necessary. Additional rounds may result in a NIST ECR Fee and possible points
952 (see section [3.2.8 Extended Cost Recovery](#)). This process continues until the CSTL receives an
953 All OK from the CMVP. Each round of comments will result in an update in the MIP List
954 Coordination date. The CSTL must respond within 90 days to prevent the review from being
955 placed on hold. Also, see [Section 4.4.6](#) *Changes while in Coordination* for more information.

956 4.1.1.5 Finalization

957 The FINALIZATION stage focuses on assuring any changes during the coordination phase have
958 been updated by the CSTL and confirm the vendor and module information is accurate. If any
959 changes are necessary, another finalization review will be performed. With the successful
960 completion of the submission review, the validation is posted on the CMVP website.

961 4.1.1.6 Validation Certificate

962 Once the information is confirmed, the Validation Authorities, issue a certificate number which
963 is added to the database. The web-based search tool for the database can be found at
964 [https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search)
965 [modules/Search](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search). The entry includes the version number of the validated cryptographic module
966 and the benchmark configuration of the original validation testing.

967 The information on the certificate pertains to the module from the time of its validation. During
968 the validation life cycle, information for that validation may change. For revalidations that do not
969 create a separate validation number, the module's validation will be updated on the website and
970 the dates of the updates and the CSTLs that submitted the updates are appended to the entry.
971 Therefore, users should refer to the NIST website for the latest information concerning a
972 validation. A Consolidated Validation Certificate (CVC) is generated at the end of each month
973 which lists all of the certificates that were published during the month. CCCS and NIST sign the
974 CVC listing and it is posted as a link on each of the individual module validation entries.

975 4.2 Implementation Under Test (IUT) and Modules in Process (MIP)

976 The *CMVP Implementation Under Test (IUT) and Modules In Process (MIP) Lists* are provided
 977 for information purposes only. Participation on the lists is *voluntary* and is a decision made by
 978 the vendor. Modules are displayed alphabetically by name, but the list doesn't necessarily
 979 include all modules being tested or reviewed.

980 The IUT List is a way to identify modules that are currently under contract to be tested by a
 981 CSTL. The List provides the module name, vendor name, FIPS 140 standard, and the date of the
 982 last update.

983 The [Modules In Process \(MIP\) List](#) only includes scenarios that result in issuing a new certificate
 984 (i.e., Full Submission (FS), Update (UPDT), Rebrand (RBND), Port Sub Chip (PTSC),
 985 Algorithm Transition (TRNS)). The status of these submissions can be tracked through the MIP
 986 List. The List includes the module name, vendor name (and expandable contact information),
 987 FIPS 140 standard, current MIP state, and the date of the last MIP state change. Any module that
 988 the vendor does not choose to be made public will be reflected at the end of the list in the "Not
 989 Displayed" row without any identifying information.

990 The IUT and MIP Lists are explained and accessible on the NIST webpage
 991 <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process>.

992 Note: Posting on either list does not imply or guarantee FIPS 140 validation.

993 4.3 Validation Submission Queue Processing

994 4.3.1 Full and Update Submission Validations

995 Modules submitted for initial validation (FS) and those submitted with less than 30% security
 996 changes (UPDT) will be queued together and addressed on a first-come, first-serve basis. All
 997 submissions in this queue must meet all requirements as of the submission date. The internal
 998 review disposition of a module report is left to the sole discretion of the NIST and CCCS CMVP
 999 program managers. Vendors should contact their CSTL for additional queue status.

1000 In cases whereby submissions are related to or dependent on other submissions, e.g., bound or
 1001 embedded modules, the CMVP must be notified for consideration prior to their submission.
 1002 CSTLs should also include this information in the special instructions field in Web Cryptik. This
 1003 will allow CMVP to manage resources in support of these larger efforts. In general, and for
 1004 dependent or related modules, testing must be completed prior to submission (including FIPS
 1005 140-3 compliance testing and CAVP/ESV validations). In addition, prior to completion, the
 1006 CSTL must review and address all changes from the completed validation.

1007 4.3.2 All other submissions

1008 The CMVP internally maintains separate queue(s) to maximize throughputs for all other
 1009 submissions, which are expected to require less review effort and faster turnaround.

1010 4.3.3 Request for Transition Period Extension

1011 Some Implementation Guidance is assigned a transition period before compliance to this
 1012 guidance is required; e.g., since meeting the guidance may require changes to cryptographic
 1013 modules or the functional testing of them as opposed to documentation changes. In rare
 1014 circumstances, the transition period may not be long enough for the vendor to perform the
 1015 modifications needed to the cryptographic module for it to be compliant with the issued
 1016 Implementation Guidance nor complete the additional cryptographic algorithm validation testing
 1017 before the scheduled date for submission of the validation report.

1018 These situations will be reviewed on a case-by-case basis at the request of the CSTL performing
 1019 the validation testing. A ruling will be made by the CMVP as to whether an extension can be
 1020 granted for this particular requirement, for this particular cryptographic module, depending on
 1021 the type of cryptographic module and the status of the validation testing.

1022 4.3.4 HOLD Status for Cryptographic Modules on the Modules In Process

1023 While a CSTL may request a HOLD, the status can be executed by the CMVP. There are several
 1024 reasons that a submission review may be placed on HOLD status. Some of these reasons are as
 1025 follows:

- 1026 1. If a module test report is sent incomplete or is determined to be incomplete once the
 1027 module has moved to the IN REVIEW or a later stage-
- 1028 2. When the ECR notification is sent to the CSTL, the module will be placed on HOLD. If
 1029 the ECR has been paid and the CSTL resubmits the report, the HOLD is removed.
- 1030 3. If a non-compliance is discovered during the module review or coordination.
- 1031 4. If a module is dependent on the completion of another module (i.e., the case of
 1032 bound/embedding), the dependent module may be placed on HOLD until the base
 1033 validation has been completed. The CSTL must indicate the module dependency upon
 1034 submission via Web Cryptik Special Instructions. If a submission is put on HOLD due
 1035 to dependency, it is the responsibility of the CSTL to notify the CMVP when the initial
 1036 submission is completed. This assures the CMVP will remove the hold for related or
 1037 dependent submissions.
- 1038 5. During COORDINATION, CMVP comments are sent to the CSTL and if the CSTL has
 1039 not responded within 90 calendar days, the module will be placed on HOLD. After 150
 1040 calendar days, an email notification will be sent to indicate that if no submission is
 1041 received in the next 30 calendar days (180 calendar days in total), the module will be
 1042 dropped from the CMVP queue. The CSTL must inform the vendor of the CMVP's
 1043 intent to drop the module due to the 6-month period of delay. If the CSTL cannot
 1044 respond to the CMVP Coordination comments within the allotted timeframe, the CSTL
 1045 must send an email justification to the CMVP identifying the reason for this delay at
 1046 least two weeks prior to the drop date. The CSTL must include a timeline specifying the
 1047 expected submission date for the CMVP's consideration. If no justification is received,
 1048 the module will be dropped. A new submission could be sent once this module has been
 1049 dropped but this would be a new submission and cost recovery would be applicable.

1050 6. A CSTL has been placed in a suspension status by NVLAP. Work in progress may be
 1051 placed in a HOLD until the suspension is lifted. No new work is allowed to be
 1052 submitted during a period of suspension.

1053 A module on HOLD will be reflected on the MIP List as “On Hold” with the date of status
 1054 change. Once the HOLD is lifted, the MIP entry will return to its prior state and queue position.
 1055 If an ECR is applicable, the ECR must be resolved, and any payment assigned must be paid
 1056 before the HOLD can be removed.

1057 4.3.5 Resubmission while in Review Pending

1058 An updated submission may be provided to the CMVP while in review pending if all the
 1059 following rules are met:

- 1060 1. This is not to be used as a placeholder, and the initial submission must have been the
 1061 intended version on the specified environment to be validated. Penalties (e.g., ECR, or
 1062 drop the module queue position) may be applied if misused. Acceptable (non-
 1063 exhaustive) examples include:
 - 1064 a. Code changes that strengthen the module’s conformance claim (e.g., improve the
 1065 granularity of the module’s show version service, or reduce potential ambiguity
 1066 with the module’s approved service indicators).
 - 1067 b. Changes under [Section 4.4.6](#) number 1 (a, b, and c).
- 1068 2. The updates must be allowed by and within the scope of the submission scenario, and
 1069 full testing or regression testing may apply depending on the changes, following the
 1070 requirements specified in [Section 7.1 Submission Scenarios](#).

1071 The updated submission will keep its place in the queue.

1072 4.3.6 Changes while in Coordination

1073 Changes during coordination for a FS or UPDT are permitted if all the following rules are met
 1074 (subject to change, especially once additional [Section 7.1 Submission Scenarios](#) become
 1075 available in Web Cryptik):

- 1076 1. Changes are limited to one or more of the following:
 - 1077 a. Quality / documentation updates to address CMVP checklist items or lessons
 1078 learned from other module validations. Documentation improvements are
 1079 encouraged to ensure accurate, high-quality reports and avoid ECR.
 - 1080 b. In direct response to CMVP comments.
 - 1081 c. Changes known at the time that would normally fit under: [CVE](#) or other
 1082 vulnerability, [NSRL](#), [TRNS](#), [VUP](#), [VAOE](#), [OEUP](#)¹, and/or [ALG](#). The
 1083 requirements for these submission scenarios must be met per [Section 7.1](#)

¹ Only permitted on a case-by-case basis with proper justification provided to the CMVP in advance of the resubmission. Considering the complexities of adding OEs, the CMVP may end up rejecting the proposal during Coordination and require adding OEs after the module has first been validated.

1084 [Submission Scenarios](#) (e.g., limited changes, regression testing, CAVP/ESV
1085 testing, etc.).

1086 2. A detailed change summary needs to be provided to the CMVP for all changes that are
1087 outside 7.1 Submission Scenarios (this is expected to be part of the Comment document
1088 itself). For changes specific to the 7.1 Submission Scenarios, a separate Revalidation
1089 Change Document is required per [7.1.1](#).

1090 Notes:

- 1091 a. Updates to improve documentation is encouraged to ensure accurate, high-quality reports
1092 and avoid ECR.
- 1093 b. The review may be delayed for complexity (time incurred) depending on the impact of
1094 the changes.
- 1095 c. Post-validation (once supported by the CMVP), additional changes can be made using the
1096 revalidation scenarios per [Section 7.1](#) of this document.
- 1097 d. Code changes will impact compliance to AS04.13 due to new versioning.

1098 4.3.7 Validation Deadline

1099 CMVP may drop modules from the queue that have not completed the validation process within
1100 2 years of being placed in IN REVIEW status. Should the modules approach the 2-year deadline,
1101 CSTLs have the option to contact the CMVP for reconsideration; CMVP will consider factors
1102 that contribute to the delay (e.g. if the delay was not due to CSTL or vendor unresponsiveness /
1103 inadequacy in addressing CMVP comments in a timely and efficient manner). When the module
1104 is dropped, the vendor and lab must restart the validation process including paying a new cost
1105 recovery fee at the current rate. This applies to all submissions currently in the process as well as
1106 to new submissions.

1107 4.4 Validation when Test Reports are not Reviewed by both Validation Authorities

1108 On rare occasions, laws from either country or other unusual circumstances prevent the release
1109 of product information outside its borders for specific products. In those occasions, both
1110 Validation Authorities will be advised of the circumstances, and the Validation Authority from
1111 that country will carry out the validation process on its own and present the certificate to the
1112 other Validation Authority for its signature (where applicable).

1113 4.4.1 Controlled Unclassified Information

1114 If a CMVP test report is received from a CSTL and it is identified in the signed letter of
1115 affirmation that it is subject to the International Traffic in Arms Regulations² (ITAR), the

²Example: Not Releasable to Foreign Persons or Representatives of a Foreign Interest.

INFORMATION SUBJECT TO EXPORT CONTROL LAWS of the UNITED STATES of AMERICA

Information subject to the export control laws. This document, which includes any attachments and exhibits hereto, may contain information subject to the International Traffic in Arms Regulation (ITAR) or Export Administration Regulation (EAR). This information may not be exported, released, or disclosed to foreign persons inside or outside the United States without first obtaining the proper export authority. Violators of ITAR or EAR are subject to civil and

1116 following CMVP programmatic guidance will be adhered to:

1117 4.4.1.1 CMVP ITAR Guidance

- 1118 1. Report submission as specified in Web Cryptik applies and should include the following
1119 changes from a normal submission:
- 1120 a. A proprietary security policy [PDF] submitted in lieu of a non-proprietary
1121 security policy.
 - 1122 b. Provide a signed letter of affirmation from the vendor stating the applicability
1123 of ITAR to the submitted test report.
 - 1124 c. To satisfy binding of Cryptographic Algorithm Validation Certificates, (see [IG](#)
1125 [2.3.A](#)), the test report must affirm that the CSTL has PDF images (front and
1126 back) for any ITAR cryptographic algorithm validation certificates, where the
1127 algorithm website will not have any detailed information.
 - 1128 d. The test report package is submitted only to NIST CMVP. The TID field will
1129 be formatted as: TID-*nn-nnnn*-ITAR. The characters ITAR will replace the
1130 field that was allocated for the CCCS TID.
 - 1131 e. Actual module names, version numbers, and vendor information will be
1132 provided. This information will not be masked by dummy information.
- 1133 2. Report review
- 1134 a. Each ITAR report will be reviewed by NIST reviewers only.
- 1135 3. Certificate generation and posting
- 1136 a. Certificates will be prepared by NIST only.
 - 1137 b. Certificates will be signed only by NIST. The CCCS signature field will be
1138 marked as: Not Applicable – ITAR.
 - 1139 c. The NIST CMVP web page will only post the following information:
1140 Certificate number, applicable FIPS standard, Status, Module Type,
1141 Embodiment, Validation Date, Sunset Date and Overall Level. It will also
1142 include the testing Lab and associated NVLAP Code.
 - 1143 d. The official certificate will be sent to the CSTL for presentation to the vendor.
- 1144 4. Re-validation
- 1145 a. All re-validation changes will result in a new certificate sent to the CSTL for
1146 presentation to the vendor since the web site will not have any identifiable
1147 information.
 - 1148 b. Report submission, report review, certificate generation and posting as outlined
1149 above and following the submission requirements.

1150 **4.5 CMVP Fees³**

1151 4.5.1 Cost Recovery Program (CR & ECR)

1152 Fees are charged to the CSTL by NIST CMVP to offset the cost of the validation authority
 1153 activities performed by NIST CMVP. Cost Recovery (CR) fees are collected depending on the
 1154 submission scenario as listed in Submission Scenarios. Extended Cost Recovery (ECR) fees are
 1155 collected when the submission review exceeds the allotted resources and/or the submission
 1156 results in one of the categories in [3.2.8 Extended Cost Recovery](#). The ECR fee is billed separately
 1157 from any applicable CR fee.

1158 Fees charged by NIST as part of the cost recovery program are listed at:

1159 <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees>.

1160 Review of submissions will not begin until NIST CMVP receives confirmation that the invoice
 1161 has been paid. CR fees cannot be reimbursed after the submission has entered the In-Review
 1162 phase.

1163 4.5.2 NIST Payment Policy

1164 Only CSTLs with an active CRADA agreement can be invoiced. NIST CMVP maintains the
 1165 billing information for each CSTL. If the CSTL's information needs to be updated (e.g., [CSTL](#)
 1166 [relocation](#)), contact NIST CMVP. Upon receipt of the CSTL's submission or a request for an
 1167 invoice, NIST billing (a separate office of NIST) prepares an invoice and submits it to the
 1168 identified payee. For questions about methods of payments and associated handling fees contact
 1169 NIST Billing Information: 301-975-3880 or at billing@nist.gov. In the event a cost recovery
 1170 refund is warranted, the request must be directed to cmvplab@nist.gov.

1171 4.5.3 Invoice for a Report Submission

1172 The CR process is initiated upon receipt of the report submission or can be initiated before the
 1173 report submission.

1174 To initiate the CR process, the CSTL must send an IUTA (IUT-Add) using Web Cryptik
 1175 indicating the correct number of modules, overall security level, and submission type. The IUTA
 1176 can be submitted without requesting that the module be placed on the IUT List. The IUTA must
 1177 be successfully processed by the NIST CMVP automated system. When the submission is
 1178 successfully processed, the CSTL will receive an automated response, "*Thank you for your*
 1179 *submission*".

1180 At any time after the CSTL receives the automated response to the IUTA, the CSTL has the
 1181 option to send an IUTB (IUT-Billing) to initiate the CR process before submitting the report.
 1182 When the IUTB is successfully processed, the CSTL will receive an automated response.
 1183 Changes to the overall security level and submission type will not be accepted.

³ CCCS does not levy any charges for the validation of cryptographic modules.

- 1184 o If the CSTL sends an IUTB and then needs to cancel the invoice, the CSTL must send
 1185 an IUTC (IUT-Cancel billing). When the IUTC is successfully processed, the CSTL
 1186 will receive the automated response.
 1187 o Once the invoice has been paid, the payment may be refunded if the module submission
 1188 is dropped prior to the IN REVIEW stage.
 1189 o Only the module.json file is required for an IUTB or IUTC. For more information on
 1190 this process, see the Web Cryptik help and User Guide.

1191 Labs should note when the cost recovery process starts, no changes to the Security Level or
 1192 Submission Type will be accepted. In addition, if a report has not been received by 90 days after
 1193 the IUTB was accepted, the module will be moved to On Hold and removed from the IUT List.
 1194 The module can be automatically removed from On Hold and placed on the MIP List by sending
 1195 the report. If the lab chooses to not send an IUTB, the CR process will initiate upon receiving the
 1196 report submission.

1197 **4.6 Flaw Discovery Handling Process**

1198 When a flaw is discovered in a **validated** cryptographic module and brought to the attention of
 1199 the CMVP Validation Authorities, the following actions will be taken:

- 1200 1. NIST, CCCS and the CSTL will investigate the allegation about the flaw, and
 1201 determine its impact on the validation;
- 1202 2. NIST and CCCS will decide whether the flaw requires the revocation of the
 1203 validation, a caveat be placed on the entry in the *Cryptographic Module Validation*
 1204 *List*, or no action;
- 1205 3. NIST and CCCS may notify NVLAP about the possible shortfall in the
 1206 CSTL's proficiency.

1207 The diagram found in Annex A outlines the flaw discovery handling process. There are several
 1208 ways for a flaw to be identified including a security-relevant CVE from the National
 1209 Vulnerability Database (NVD).

1210 **4.7 Historical or Revoked Validations**

1211 **Historical** – Agencies may make a risk determination on whether to continue using this module
 1212 based on their own assessment of where and how it is used. For more details, please visit the
 1213 CMVP webpage: [https://csrc.nist.gov/Projects/cryptographic-module-validation-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules)
 1214 [program/validated-modules](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules)

1215 If the validation certificate is historical, it will appear on the *CMVP Validation List* with the
 1216 validation status *Historical*.

1217 Examples that may result in a FIPS 140 validation being made historical by the CMVP:

- 1218 • A validation implements cryptographic algorithm(s) in the approved mode that are no
 1219 longer approved (e.g., an algorithm transition date has passed that was identified as one
 1220 that will move the module to the historical list per the CMVP [Programmatic Transitions](#)
 1221 webpage).

- 1222 • Sunset date as shown on the validation is reached.
- 1223 • A validation is bound to or embeds another validation that moved to the historical list
- 1224 (e.g., due to being sunset or an algorithm transition).

1225 If an issue with a validation is discovered by the vendor or CSTL, the CMVP must be notified of

1226 the issue with a proposed schedule of when a correction will be submitted to the CMVP. The

1227 CMVP will consider the severity of the issues, the proposed timeline for correction, and if the

1228 issue was proactively requested (which is greatly encouraged/supported) when determining if the

1229 validation should be revoked or made historical. E.g., the CMVP may decide to keep the

1230 validation on the Active list until the revalidation submission that addresses the issue is

1231 completed.

1232 The revalidation submission will either result in the same certificate being updated (whereby no

1233 further CMVP action needed), or it will result in a new certificate number in which case the

1234 original certificate may then be moved to the historical or revocation list. The CMVP may move

1235 the module to the historical or revocation list if the corrections are not made in a timely manner.

1236 **Revoked** - The module validation is no longer valid, and this certificate may not be referenced to

1237 demonstrate compliance to FIPS 140-3.

1238 If the validation certificate is revoked, it will appear on the *CMVP Validation List* with the

1239 validation status *Revoked*.

1240 Examples that may result in a FIPS 140 validation being revoked by the CMVP:

- 1241 a. Discovery of a security non-compliance or security flaw in a validated cryptographic
- 1242 module (typically one that would require module code changes to correct).
- 1243 b. Discovery that the cryptographic module was validated using false information.
- 1244 c. A CVE is discovered, and the module has been updated to mitigate the CVE. The
- 1245 module version with the CVE may be removed from the validation on the completion of
- 1246 the CVE submission which is effectively the same as revoking the validation for that
- 1247 version (see [7.1.11 CVE](#) for more information).
- 1248 d. Significant documentation issues that have a security impact to the operator of the
- 1249 module such as incorrect claims to:
- 1250 ○ Any of the items in [7.8 Module definitions for same certificates](#),
- 1251 ○ Module Caveat,
- 1252 ○ Tested Configuration(s),
- 1253 ○ Versions (i.e., Software, Firmware, or Hardware),
- 1254 ○ Other CMVP documentation requirements (e.g., in IGs, MM, and SP 800-140
- 1255 series) that have a security impact on the operator.

1256 **4.8 Entropy Source Validation (ESV) Processes**

1257 In April 2022, the CMVP introduced a new submission process for entropy sources leading to

1258 standalone entropy source validation certificates. The validation certificates provide the

1259 assurance that a particular entropy source on a particular operating environment conforms to SP
1260 800-90B and associated IGs.

1261 Similar to ACVTS, the CMVP maintains two environments: a Demo ESVTS, and a Prod
1262 ESVTS. The Demo environment is for testing and becoming familiar with the platform. The
1263 Prod environment is for certification.

1264 Prod ESVTS is the only mechanism the CMVP allows on a new submission that requires a
1265 validation on an entropy source. Entropy source validation will no longer be accepted as part of a
1266 module submission (i.e., designated as ENT on the module certificate). Instead, the module
1267 submission must cite an existing entropy validation certificate. See Section 7.1.14 for additional
1268 information on ESV and ENT claims.

1269 4.8.1.1 Entropy Source Validation Submissions

1270 To submit to ESVTS, a client must be used to interact with the server. The CMVP provides two
1271 clients for use: an HTML-based WebClient, and a Python client. Both have their advantages and
1272 features. It is encouraged that a lab is familiar with both options.

1273 Several files are expected to be included in the submissions. It is the best practice to have these
1274 ready before making the initial request to ESVTS. The minimum set of files are as follows:

1275 1. Entropy Assessment Report (EAR) – This file addresses the requirements in SP 800-
1276 90B and describes how the entropy source on the listed operating environments conforms
1277 to the standard and associated IGs.

1278 2. Public Use Document (PUD) – This file provides information to a user that may
1279 incorporate or use the entropy source within a cryptographic module.

1280 3. Data Collection Attestation (DCA) – This file addresses the SP 800-90B Section 3.2.4
1281 requirements. The document must contain the name of each operating environment tested
1282 in this manner and a signature from the vendor representative. This file is optional,
1283 depending on how the data was collected from the entropy source. It may also be attached
1284 to the EAR instead of provided separately.

1285 4. Data Files – These are files described in SP 800-90B that capture outputs from the
1286 entropy source. The files are subject to the SP 800-90B Entropy Assessment Tool available
1287 on GitHub. The number of files required depends on the entropy source being evaluated.

1288 Part of the certify step (which is the last step of the submission to the ESVTS) is the inclusion of
1289 an Entropy Identifier (EID) that will help the lab track the submission as it goes through the
1290 review process. The EID must be four alphanumeric characters and must not repeat with
1291 previous EIDs used by the lab. This is similar to the TID used within the module review process.
1292 A string used as an EID may still be used as a TID and vice versa.

1293 After a submission is sent for certification the CMVP will perform cost recovery before the
1294 submission is passed along for manual review. During the manual review, two CMVP entropy
1295 reviewers will confirm the documentation provided addresses all of the SP 800-90B
1296 requirements.

1297 If the ESV submission is designated as ITAR:

- 1298 a. Provide a signed letter of affirmation from the vendor stating the applicability of ITAR
 1299 to the submitted report.
 1300 b. Use a client to submit the entropy assessment to the API and upload the corresponding
 1301 data files. The description field can be modified.
 1302 c. Use nfiles to send the EAR, PUD, DCA, JSON metadata for ACVTS, and entropy
 1303 assessment ID(s) to Chris Celi, christopher.celi@nist.gov.
 1304 d. Comment responses go ONLY to cmvpitar@nist.gov using PGP encryption. There is no
 1305 ITAR flag in the EID.
 1306

1307 An ESV certificate has a reuse status of either “Reuse restricted to vendor” or “Open for reuse”.

1308 “Reuse restricted to vendor” means:

- 1309 a. Any module that has the same vendor can use the ESV certificate within their module
 1310 with no additional permission, if the entropy source is portable to that module per the
 1311 PUD guidance (e.g., identical environments, configuration steps, etc.).
 1312 b. The vendor’s name of the ESV certificate must match exactly with the module vendor
 1313 name, unless the two vendors are part of the same company (e.g., different divisions with
 1314 slightly different names, or a company is a subsidiary of another company that has a
 1315 validation). This vendor relationship would need to be explained with evidence provided
 1316 to the CMVP as part of the module submission.
 1317 c. Someone other than the vendor can only use the certificate with written and signed
 1318 permission from the vendor’s point of contact (as indicated on the ESV certificate). The
 1319 signed permission may be appended to the PUD of the certificate or be a separate
 1320 document attached to the module submission package.

1321 “Open for reuse” means any vendor can use that certificate within their module without any
 1322 specific permission from the ESV certificate vendor. It does NOT mean the vendor can rebrand
 1323 the ESV as their own.

1324 4.8.1.2 Entropy Source Validation Web Client

1325 The WebClient provides forms that guide a submitter through the process. All information must
 1326 be submitted at once including the EAR, PUD, and raw data files. Once a request is submitted to
 1327 NIST, the user is expected to store the resulting output presented by the WebClient at the end of
 1328 the submission. This provides a way to follow up on the request if needed. The URL to access
 1329 the WebClient is the base URL of the ESVTS environment. The WebClient is available for both
 1330 Demo and Prod.

1331 4.8.1.3 Entropy Source Validation Python Client

1332 The Python Client provides a more automated way of submitting data to ESVTS. Requests may
 1333 be made piecemeal when information becomes available. The user is expected to store the
 1334 outputs from the tool. The tool automatically logs important information. The Python Client is
 1335 controlled with JSON files to drive the functionality needed at the time. This allows a user to
 1336 start making requests and pick them back up later. Configuration JSON files control if the

1337 Python Client is accessing Demo or Prod. The Python Client can be downloaded from the URL
1338 indicated in the Entropy Source Validation Webpages (Section 4.8.3)

1339 4.8.2 Entropy Source Validation Comment Remediation Process

1340 When an entropy source submission is picked up for review, the lab will receive an email about
1341 the change in status of the submission. The reviewers will evaluate the claims made in the EAR,
1342 and evaluate the information provided in the PUD. If there are questions or comments about the
1343 submission, a file will be sent to the lab with PGP-encrypted email for further clarification. The
1344 email will have the subject line “EID-XX-YYYY-[{transaction code}](#)-yyMMddHHmm” where XX is the
1345 lab code, and YYYY is the four-character EID provided during the certification request. On
1346 emails from the CMVP to the lab, the transaction code will be “CCOM#” where # is the number
1347 of comment rounds. For responses back to the CMVP, the lab must include the same subject line,
1348 but the transaction code must be “LCOM#” where the # matches the latest number sent from the
1349 CMVP. Only the changed files are required in the response email.

1350 Any ESV submission that has substantial errors or requires significant additional review effort
1351 by the validators (e.g., due to issues with quality or complexity) will be subject to a NIST ECR
1352 (see HB 150-17 H.3.4.2).

1353 4.8.3 Entropy Source Validation Webpages

1354 For more information about the ESV Process, see [https://csrc.nist.gov/Projects/cryptographic-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations)
1355 [module-validation-program/entropy-validations](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations).

1356 The ESV Certificate List is available on CSRC. See [https://csrc.nist.gov/Projects/cryptographic-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations/search)
1357 [module-validation-program/entropy-validations/search](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations/search).

1358 For access to the Python Client and ESVTS on Demo or Prod, see
1359 <https://github.com/usnistgov/ESV-Server>.

1360 4.9 CMVP Webpages

1361 This section provides information about the CMVP program that can be found on the web.

1362 4.9.1 Official CMVP Website

1363 The official CMVP website with all current publicly-available information on the CMVP is
1364 <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program>. It can also be reached
1365 through <https://nist.gov/cmvp>.

1366 4.9.2 Cryptographic Module Validation Lists

1367 The official CMVP website can generate the following lists related to the validation of
1368 cryptographic modules:

- 1369 • [Modules In Process](#) – A listing of the modules currently being reviewed by CMVP
1370 and the review state of each module. For more information about the MIP List, see

- 1371 [section 4.2.](#)
- 1372 This list is updated as additional information is available. The validation process is a
1373 joint effort between the CMVP, the CSTL and the vendor and therefore, for any given
1374 module, the action to respond could reside with the CMVP, the lab or the vendor. This
1375 list does not provide granularity into which entity has the action.
- 1376 • [Implementation Under Test](#) – A listing of the modules currently being tested at the
1377 CSTL. This list is provided by the CSTLs and includes module name, vendor, FIPS
1378 140-2 or FIPS 140-3, and the date when added to the list.
- 1379 This list is updated as information is available. The IUT is under the control of the
1380 CSTL and the vendor. The CMVP is not aware of the submission schedule for these
1381 modules under testing.
- 1382 • *Cryptographic Module Validation Search can be found at:*
1383 [https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search)
1384 [modules/Search](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search)
 - 1385 - A basic search supports a single overall list or a list resulting from a
1386 combination of vendor, module name, or certificate number. The basic search
1387 only addresses active modules.
 - 1388 - An advanced search will generate a single list with the following options:
 - 1389 • Certificate Number:
 - 1390 • Vendor:
 - 1391 • Module Name:
 - 1392 • Standard: (FIPS 140-1, FIPS 140-2, or FIPS 140-3)
 - 1393 • Module Type:
 - 1394 • Validation Status: (Active, Historical, or Revoked)
 - 1395 • Embodiment:
 - 1396 • Year Validated:
 - 1397 • Overall Security Level:
 - 1398 • Algorithm:
 - 1399 • Allowed Algorithms:
 - 1400 • Tested Configuration:
 - 1401 • Caveat:
 - 1402 • Hardware Versions:
 - 1403 • Software Versions:
 - 1404 • Firmware Versions:
 - 1405 • Lab:
- 1406 The search list is updated when new validation certificates are posted to the
1407 website. Only the current validation information is shown, however, changes are
1408 indicated in the validation history.
- 1409 The lists are being improved as needs and time allows, so that more information
1410 than indicated here may be available from these sources before the next update of
1411 this document.

1412 4.9.3 CMVP Certificate Page Links

1413 Once the validation is identified, the information displayed typically includes vendor
1414 information, module information, and required caveats. For each certificate there are also several
1415 links from these pages that may be useful. These are described below.

1416 4.9.3.1 Security Policy

1417 This link is connected to the security policy that is the summary of the capabilities and security
1418 information of the module in a PDF format. The file is created under the agreement from the
1419 vendor and is available from the CMVP website.

1420 4.9.3.2 Consolidated Validation Certificate

1421 This link is connected to a list of certificates that were issued for the month of interest. It
1422 provides summary information that is accurate at the time of signing. For the latest module
1423 information, please refer to the certificate page. The file is created by CMVP and is from the
1424 CMVP website. Recent validations may not have this link available.

1425 4.9.3.3 Vendor Link

1426 This link is provided by the vendor to CMVP. The vendor is responsible for the accuracy of the
1427 link and the content. The CMVP does not endorse the views expressed or the information
1428 presented in the directed link, nor does it endorse any commercial products that may be
1429 advertised or available at the directed link.

1430 4.9.3.4 Vendor Product Link

1431 The purpose of this web link is for vendors to provide a concise listing of known products which
1432 incorporate their validated cryptographic module or, if the cryptographic module is a standalone
1433 product, additional relevant information about the product. The CMVP hopes that this link will
1434 make it easier for potential customers and users to identify products that use validated
1435 cryptographic modules.

1436 The link in the certificate details page is to a vendor provided URL that is vendor created and
1437 vendor maintained. The provision of this Vendor Product Link by the vendor is optional. The
1438 CMVP does not endorse the views expressed or the information presented in the directed link
1439 nor does it endorse any commercial products that may be advertised or available at the directed
1440 link. Press releases are not accepted.

1441 4.9.3.5 Algorithm Certificates

1442 Links to the CAVP validation certificate for the approved algorithms used in the module are
1443 provided for those wishing to know more details to the specific testing performed. The link is
1444 from the CAVP website. This currently is under development and may change. Algorithm
1445 validation certificates can also be found in the security policy.

1446 4.9.3.6 Validation History

1447 The initial validation and all updates are shown along with the CSTL responsible. The validation
1448 shown includes all updates and is considered the official validation. If information concerning a
1449 revalidation is needed, contact the CSTL indicated on the validation certificate.

1450 4.9.4 Usage of FIPS 140-3 Logos

1451 Once validation is achieved CMVP will forward through the CSTL to the Vendor instructions
1452 about the use of the NIST FIPS 140-3 logo. Vendors who use validated modules in their products
1453 may also request use of the NIST FIPS 140-3 Logo. The request instructions and use
1454 requirements is available from the CMVP web site: [https://csrc.nist.gov/Projects/cryptographic-
1455 module-validation-program/use-of-fips-140-2-logo-and-phrases](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/use-of-fips-140-2-logo-and-phrases). Completed forms are sent to
1456 cmvp@nist.gov.

1457 **5 CMVP and CAVP Programmatic Metrics Collection**

1458 This section provides an overview of the CMVP and CAVP Programmatic Metrics Collection
1459 and a description of the collection and reporting processes of the CMVP metrics.

1460 **5.1 Overview**

1461 The CMVP Programmatic Metrics Collection process is intended to document the quality
1462 performance of the testing and validation processes of the CMVP and to allow the program to
1463 evaluate its relevance within the government. To achieve these objectives various metrics are
1464 collected through the testing and validation processes of the CSTLs and the CMVP. These
1465 metrics are intended to identify general programmatic trends and not to measure individual
1466 CSTL or vendor performances.

1467 **5.2 Confidentially of the Collected Metrics Data**

1468 The CMVP considers the data collected and reported by the individual CSTLs as proprietary.
1469 CMVP makes every effort to anonymize the information by sampling only larger data sets and
1470 combining them without tracking information. The statistical information derived from the
1471 collected data is considered to be non-proprietary.

1472 **5.3 Collected Metrics**

1473 With the migration to FIPS 140-3 and the changes in the collection tools, the CMVP are
1474 currently reevaluating the methods used to collect useful metrics. Though the program may
1475 follow much of the previous procedures, it is not possible at this time.

1476 6 Test Tools

1477 This section covers the testing tools CSTLs are expected to utilize in the testing and reporting of
 1478 validation submissions. Where applicable, the title of the person responsible for the update
 1479 and/or maintenance of the document is identified.

1480 6.1 Web Cryptik

1481 Web Cryptik is a required tool for the completion of module testing, and generation of
 1482 documents that must be included in a formal submission from the CST. The Web Cryptik tool is
 1483 to be used to record details of the cryptographic module being tested, the specific testing
 1484 performed, and the results of the validation testing. It is also to be used to create, among other
 1485 documents, the FIPS 140 validation test report. Information about new features, enhancements,
 1486 and bug fixes are provided with each release of the tool in the Web Cryptik User Guide.

1487 The CMVP encourages suggestions, fixes, and improvements posted to the Github page
 1488 <https://github.com/usnistgov/CMVP/issues> following the labels provided
 1489 <https://github.com/usnistgov/CMVP/labels>.

1490 Most submissions to CMVP are done through the use of Web Cryptik. The Web Cryptik User
 1491 Guide provides a summary table of the submissions supported by Web Cryptik and files that
 1492 must be included with the submission.

1493 **Responsible Individual:** NIST CMVP Program Manager.

1494 6.2 Suggested Tools for Physical Testing

1495 As indicated in HB 150-17 Section B.6.4.2, a CSTL must meet the minimum hardware and
 1496 software requirements for physical security testing. The CSTL can determine which tools to use
 1497 to meet the requirements. All measurement equipment used to meet specific criteria in the
 1498 conformance testing must have a valid calibration certificate from a separate accredited
 1499 calibration laboratory. All equipment with storage capabilities must meet CSTL security
 1500 policies. Personal equipment is prohibited for use in testing.

1501 Below are some examples of tools for physical testing:

1502 X-Acto or Utility "Type" knives (including various blades)
 1503 Strong artificial light source (Wavelength range of 400nm to 750nm)
 1504 Magnifying glass
 1505 Dremel "Type" Rotary Tool (including accessory bits: cutting, grinding, drilling, carving,
 1506 etc.)
 1507 Jeweler's screwdrivers (e.g., flat, phillips, robertson, torx, hex key)
 1508 Dentist "Type" Instruments (e.g., picks and mirrors)
 1509 Razor Saw
 1510 Small pliers (e.g., needle nose, standard nose, long nose, curved nose, side cutters)
 1511 Hammer
 1512 Chisels
 1513 Fine (small) files
 1514 Heat Gun or Heat Source

- 1515 Spray Coolant
- 1516 Digital camera (personal phones are not acceptable)
- 1517 Digital scanner
- 1518 Printer
- 1519 ANSI C Compiler
- 1520 Debugger or binary editor
- 1521 Microsoft Office Professional
- 1522 Adobe Acrobat Standard
- 1523 Personal protection equipment for chemical testing (e.g., goggles, gloves)
- 1524

1525 The equipment below may require calibration if used to measure to a reference:

- 1526 Volt-Ohm-Milliammeter (VOM) or Digital Multimeter (DMM)
- 1527 Variable Power Supply
- 1528 Digital Storage Oscilloscope and/or Logic Analyzer
- 1529 Temperature Chamber

1530 7 CMVP General Testing and Reporting Guidance

1531 In order for CMVP to manage the program more efficiently, additional testing requirements are
 1532 addressed below. Several of the issues that were under section G of the FIPS 140-2
 1533 Implementation Guidance are presented in this section. This guidance does not change the
 1534 cryptographic module requirements of ISO/IEC 19790:2012 but may impact ISO/IEC
 1535 24759:2017 documentation and testing requirements.

1536 7.1 Submission Scenarios

1537 An updated version of a previously validated cryptographic module can be considered for a
 1538 *revalidation* rather than a *full validation* depending on the extent of the modifications from
 1539 the previously validated version of the module. (Note: the updated version may be, for
 1540 example, a new version of an existing cryptographic module or a new model based on an
 1541 existing model.)

1542 7.1.1 Requirements for all revalidations

1543 For any revalidation, the vendor is responsible for reviewing all FIPS 140-3 requirements
 1544 and making sure any change has been addressed throughout the module requirements and
 1545 that proper documentation has been completed and submitted to the CSTL. The CSTL is
 1546 responsible for an independent evaluation of the impacts throughout the module
 1547 requirements for any change and performs any testing needed prior to submission. The
 1548 CSTL **shall** address all affected TEs and the CSTL's assessment. The details **shall** be
 1549 included in an updated Web Cryptik package with a summary of the changes listed in the
 1550 Revalidation Change Document (<https://csrc.nist.gov/projects/cmvp/sp800-140b>).

1551 For all revalidations, the Web Cryptik package **shall** include all information required by
 1552 that revalidation scenario. The ZIP file and files within the ZIP file **shall** follow the
 1553 requirements in the Web Cryptik User's Guide and be submitted to the CMVP using the
 1554 specified data protection methods. Additional documentation may be required if CMVP
 1555 guidance requiring the additional documentation has been published since the module's
 1556 original validation.

1557 All scenarios **shall** be processed and submitted to the CMVP by a CSTL.

1558 If a CSTL has been contracted to perform a revalidation for a validated module for which the
 1559 CSTL did not perform the original testing on the base module:

- 1560 a. The vendor **shall** provide the CSTL with the design documentation and
 1561 implementation (including source code, HDL, etc.) of the base validated module and
 1562 of the module that has been updated.
- 1563 b. The vendor **shall** provide the CSTL with the latest Security Policy as shown on the
 1564 base module's most recent certificate (this includes the JSON files and information
 1565 necessary to generate the Security Policy for SP 800-140Br1-compliant base
 1566 modules).

- 1567 c. The vendor **shall** provide the CSTL with the latest base module validation report
 1568 (a.k.a. Test Report) for the following revalidation scenarios: NSRL, ALG, UPDT,
 1569 CVE and TRNS. This is to ensure the new CSTL has the original tests to confirm if
 1570 regression testing is necessary in addition to the minimum required by that
 1571 revalidation scenario.
- 1572 d. The vendor **shall** provide the CSTL with the latest base module physical test report
 1573 (a.k.a. PTR) for the following revalidation scenarios: NSRL, UPDT, CVE, TRNS and
 1574 PHYS. This is to ensure the new CSTL has the original tests to confirm if physical
 1575 testing was impacted (e.g., changes to the physical enclosure or changes to firmware
 1576 that controls the physical response logic).
- 1577 e. The CSTL **shall** determine that the provided base documentation and implementation
 1578 is identical to the base validated module.
- 1579 f. The CSTL **shall** examine each modification and confirm that the change is
 1580 appropriate for the submission type (e.g., non-security relevant for NSRL).
- 1581 g. The CSTL **shall** determine that no other modifications, including unintentional, have
 1582 been made to the base module apart from what is permitted by the revalidation
 1583 scenario.
- 1584 h. The CSTL submissions **shall** meet all requirements of the revalidation scenario.
- 1585 i. The CSTL submission **shall** indicate which submission scenario is applicable and a
 1586 summary of associated changes in the Change Document.
- 1587 j. The CSTL **shall** use the Change Document format for listing the certificate
 1588 information as required by each revalidation scenario.
- 1589 k. The CSTL **shall** submit, at a minimum, what is listed in the below sections as
 1590 required by the revalidation scenario.

1591 Below are the twelve possible FIPS 140-3 submission scenarios: Full Submission (FS), Vendor
 1592 Update (VUP), Vendor Affirmed Operational Environment (VAOE), Non-Security Relevant
 1593 (NSRL), Algorithm Update (ALG), Operational Environment Update (OEUP), Rebrand
 1594 (RBND), Port Sub Chip (PTSC), Update (UPDT), Common Vulnerabilities and Exposures
 1595 (CVE), Algorithm Transition (TRNS), and Physical Enclosure (PHYS).

1596 See [section 7.1.14](#) for a summary table and submission process for each of these
 1597 submission scenarios, and [section 7.1.15](#) for additional comments.

1598 7.1.2 Full Submission (FS)

1599 The first time a new software, firmware, hardware, or hybrid module is submitted for validation.
 1600 The module **shall** meet all applicable requirements at the time of submission.

1601 If modifications are made to hardware, software, or firmware components that do not meet any
 1602 of the below revalidation criteria, then the cryptographic module **shall** be considered a new
 1603 module and **shall** undergo a full validation testing by a CSTL and submitted as a FS.

1604 7.1.2.1 Interim Validation

1605 This is a temporary measure to shorten the queue and expand the active validations. These
 1606 validations are valid for two years only but can be converted to a normal full validation (with a
 1607 5-year validation date) on the completion of an additional conversion/submission compliant to
 1608 SP 800-140Br1.

1609 Interim validations can be modified under any of the below revalidation scenarios, except for
 1610 RBND.

1611 The main difference from a normal validation is that for interim validations, the CMVP depends
 1612 more on the CSTL submission with less CMVP oversight. For more information see the CMVP
 1613 webpage: [https://csrc.nist.gov/projects/cryptographic-module-validation-program/programmatics-](https://csrc.nist.gov/projects/cryptographic-module-validation-program/programmatics-transitions)
 1614 [transitions](https://csrc.nist.gov/projects/cryptographic-module-validation-program/programmatics-transitions).

1615 7.1.3 Vendor Update (VUP)

1616 Administrative updates (e.g., updating vendor contact information, grammatical Security Policy
 1617 corrections).

1618 7.1.4 Vendor Affirmed Operational Environment (VAOE)

1619 Security policy change of vendor affirmed OEs (see [Management Manual 7.9 Vendor or User](#)
 1620 [Affirmation of Modules](#)).

1621 7.1.5 Non-Security Relevant (NSRL)

1622 Modifications are made to hardware, software or firmware components **that do not affect any**
 1623 **FIPS 140-3 security relevant items**. Per [IG 2.4.A](#), “the term *security* is not defined in the Terms
 1624 and Definitions, but, within the scope of FIPS 140-3, is determined based on the Section 6
 1625 Functional Security Objectives, and the specific Section 7 Security Requirements derived from
 1626 those objectives”. The CSTL is responsible for identifying the documentation that is needed to
 1627 determine whether a revalidation is sufficient, and the vendor is responsible for submitting the
 1628 requested documentation to the CSTL. Documentation may include a previous validation report,
 1629 design documentation, source code, source code difference evidence, FSM, security policy
 1630 differences, etc.

1631 The CSTL **shall**:

- 1632 a. Review and independently verify the accuracy of the vendor-supplied documentation and
 1633 identify any additional documentation necessary to confirm the applicability of this
 1634 revalidation scenario.
- 1635 b. Determine additional testing as necessary to confirm that FIPS 140-3 security relevant
 1636 items have not been affected by the modification.
- 1637 c. Identify the assertions affected by the modification and **shall** perform the tests associated
 1638 with those assertions. This will require the CSTL to:
- 1639 i. Review the COMPLETE list of assertions applicable to the module,

- 1640 ii. Identify, from the previous validation report, the assertions that have been
1641 affected by the modification,
- 1642 iii. Identify additional assertions that were NOT previously tested but should now be
1643 tested due to the modification, and
- 1644 iv. Review assertions where specific Implementation Guidance (IG) was provided at
1645 the time of the original validation to confirm that the module still meets the IG as
1646 it existed at the time of the original validation.
- 1647 d. Perform tests identified in b and c above (expected to at least include AS04.13 to reflect
1648 the new version(s) as a result of the code changes) on all new version(s) listed on the
1649 module’s certificate on at least one configuration of one module as defined per the
1650 module count guidance under “[MIS Field Descriptions](#)”. Additionally for
1651 software/firmware/hybrid modules, tests must be done on at least one listed OE. This
1652 assumes the new versions compile to the same binary across all modules and
1653 configurations. If new versions compile to different binaries, then each binary must be
1654 tested separately.
- 1655 i. E.g., a hardware validation has two ‘base’ modules (i.e., P/N 10 and P/N 20) that
1656 map to the following firmware components: P/N 10 uses firmware components
1657 1.0 and 2.0, and P/N 20 uses firmware components 1.1, 2.0, and 3.0 (note, the
1658 same firmware component, 2.0, is shared between both ‘base’ modules). If NSRL
1659 changes were made to firmware component 2.0 (now version 2.1) but no changes
1660 were made to firmware components 1.0, 1.1 and 3.0, it is sufficient for the CSTL
1661 to test either: 1) P/N 10 using 1.1 and 2.1, or 2) P/N 20 using 1.0, 2.1, and 3.0.
1662 This assumes firmware component 2.1 compiles to the same binary for P/N 10 as
1663 it does for P/N 20. If not, P/N 10 and P/N 20 would each need to be separately
1664 tested.
- 1665 ii. If regression testing is not performed on some versions, configurations, and OEs,
1666 then those **shall** be removed from the module’s certificate UNLESS the CSTL
1667 provides proper justification on why regression testing is not necessary for the
1668 untested versions, configurations and OEs. With proper justification, these may
1669 remain on the module’s certificate.

1670 NSRL code changes (“limited” or not) would NOT require retesting CAVP certificates (even if
1671 otherwise applicable per the CAVP [FAQ GEN.9](#)), since changes are non-security relevant and
1672 verified by the CSTL as having no impact to the algorithm implementations or how it meets
1673 CAVP testing. CAVP [FAQ GEN.11](#) may be leveraged to update the CAVP versioning
1674 information if changes are made outside the algorithm boundary but still impact the versioning
1675 on the CAVP certificate (e.g., the CAVP versioning reflects the module boundary rather than the
1676 algorithm boundary).

1677 The CSTL may send the CMVP a [Request For Guidance](#) to confirm their analysis on the non-
1678 security relevant changes prior to submission, which is expected to address at least the following
1679 questions:

- 1680 1. What changes are being proposed?
 1681 2. What is the justification that each change is considered non-security relevant? E.g.,
 1682 changes are NOT to any items from [7.8 Module definitions for same certificates](#) or other
 1683 areas that affects how the module meets the security objectives and requirements of FIPS
 1684 140-3.

1685 7.1.6 Algorithm Update (ALG)

1686 Post validation, approved security relevant functions or services for which CAVP testing was not
 1687 available (or vendor affirming was still permitted per the CMVP/CAVP transition schedule) at
 1688 the time of submission to the CMVP for validation are now CAVP-tested and are being
 1689 submitted for inclusion as an approved function or service. The CSTL is responsible for
 1690 identifying the documentation that is needed to determine whether a revalidation is sufficient,
 1691 and the vendor is responsible for submitting the requested documentation to the CSTL.
 1692 Documentation may include a previous validation report and applicable CMVP rulings, design
 1693 documentation, source code, security policy differences, etc. Code or configuration changes are
 1694 not permitted under this revalidation scenario. For example, if self-tests are required for
 1695 approved algorithms, the module must already support these self-tests. In essence, this means
 1696 that ALG can only be used when a previously vendor affirmed or allowed algorithm that was
 1697 available in the approved mode now has CAVP testing available and already meets the algorithm
 1698 requirements (e.g., self-tests) and module requirements (e.g., approved service indicator).

1699 The CSTL **shall**:

- 1700 a. review and independently verify the accuracy of the vendor-supplied documentation and
 1701 identify any additional documentation necessary to confirm the applicability of this
 1702 revalidation scenario.
 1703 b. identify the assertions affected by the modification and **shall** perform the tests associated
 1704 with those assertions. This will require the CSTL to:
 1705 i. Review the COMPLETE list of assertions applicable to the module,
 1706 ii. Identify, from the previous validation report, the assertions that have been
 1707 affected by the modification,
 1708 iii. Identify additional assertions that were NOT previously tested but should now be
 1709 tested due to the modification, and
 1710 iv. Review assertions where specific Implementation Guidance (IG) was provided at
 1711 the time of the original validation to confirm that the module still meets the IG as
 1712 it existed at the time of the original validation, except for IGs related to the newly
 1713 tested algorithm where the latest IGs **shall** be met.

1714 7.1.7 Operational Environment Update (OEUP)

1715 No changes to the module with an addition, modification, or deletion of tested operational
 1716 environments (OEs). Purely deleting OEs can be done as a NSRL, but deleting can be done
 1717 within an OEUP if also adding and/or modifying OEs. This **shall** require CAVP-testing the

1718 algorithm validations on the new/modified OEs. If an entropy source assessment is applicable
 1719 per [IG 9.3.A](#), ESV(s) to cover all new/modified OEs and/or platforms **shall** be submitted and
 1720 validated separately prior to submission. The CSTL **shall** perform the full regression test suite
 1721 shown on the [CMVP website](#).

1722 The only time code changes are allowed as part of an OEUP is if they are non-security relevant
 1723 and *necessary* to correctly run the module on the new/modified OE (e.g., compilation flags or
 1724 configuration options that need to be updated). No other changes are permitted (even to
 1725 incorporate other non-security relevant changes such as bug fixes). In Web Cryptik, this may be
 1726 captured as a checkbox under the OEUP submission scenario (e.g., the CSTL selects “Limited
 1727 NSRL”).

1728 Upon re-testing and validation, the CMVP provides the same assurance as the original OE(s) as
 1729 to the correct operation of the module on the new/modified OE(s). The new/modified OE will be
 1730 added to the module’s validation entry.

1731 As a potential alternative to an OEUP, module vendors and users may take advantage of the
 1732 porting provisions explained in [7.9 \(Vendor or User Affirmation of Modules\)](#) of this document.

1733 7.1.8 Rebrand (RBND)

1734 This scenario applies if there are no modifications to a module and the new module is a re-
 1735 branding of an already validated Original Equipment Manufacturer (OEM) module. The CSTL
 1736 **shall**:

- 1737 1. determine that the re-branded module is identical to the OEM module (n.b. this
 1738 requirement applies equally to open source and non-open-source modules).
- 1739 2. include the OEM’s written approval for re-branding in the submission package which
 1740 **shall** note the terms of permission (e.g., subsequent addition of OEs, possible re-use of
 1741 CAVP certificates, entropy, non-security relevant changes, remediation of CVE, whether
 1742 a rebrand of a rebrand is acceptable, etc.) including who owns/controls the codebase and
 1743 is responsible for updates to it post validation. E.g., if these terms do not explicitly allow
 1744 a vendor to further rebrand the OEM module, then a rebrand of that rebranded module is
 1745 not permitted unless written permission is granted by the OEM.
- 1746 3. (for modules containing any open-source licensed code) ensure the open-source licensing
 1747 requirements are met (e.g., any required notices are contained in the Security Policy).

1748 A RBND **shall** include at least one OE from the original validation and cannot add new OEs.
 1749 With proper OEM permissions, a RBND followed by a separate OEUP submission can
 1750 accomplish rebranding a module on different OEs.

1751 The only time it is allowed to combine a RBND with other scenarios is as follows:

- 1752 a. A RBND may be combined with a PHYS only if physical changes are *necessary* to
 1753 correctly rebrand the module. For example, if the paint or coating on the hardware of the
 1754 rebranded module is changed to reflect the new company's color schemes, and/or to
 1755 change the vendor and product names on the enclosure. In Web Cryptik, this may be
 1756 captured as a checkbox under the RBND submission scenario (e.g., the CSTL selects
 1757 “PHYS”).

- 1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
- b. The only time code changes are allowed as part of a RBND is if they are *necessary* to correctly rebrand the module (e.g., to display the new module name/version/logo, or to use the new vendor's color schemes/visual aesthetics). No other changes are permitted (even to incorporate other non-security relevant changes such as bug fixes). In Web Cryptik, this may be captured as a checkbox under the RBND submission scenario (e.g., the CSTL selects “Limited NSRL”).
 - c. A RBND is essentially guaranteed to be combined with a VUP to address the vendor changes so this will not be separately selectable in Web Cryptik.
 - d. A vendor is expected to have permission to reuse the OEM’s CAVP certificates. Therefore, changes to CAVP certificate information are NOT permitted as part of a RBND (but if permission is granted by the OEM, may be part of a post-RBND revalidation such as a UPDT).

1774 The CSTL **shall** provide an updated security policy which is technically identical to the
1775 originally validated security policy and describes the re-branded module.

1776 7.1.9 Port Sub Chip (PTSC)

1777 A sub-chip cryptographic subsystem that was previously validated in a single-chip (see [IG 2.3.B](#))
1778 can be ported to other single-chip constructs as a PTSC submission to the CMVP. The following
1779 is applicable to validate this new single-chip module:

- 1780
1781
1782
1783
1784
- a. The CSTL **shall** verify that there are no security relevant changes in the sub-chip cryptographic subsystem;
 - b. If an entropy source is contained within the sub-chip cryptographic subsystem, ESV(s) to cover all new single-chip environments **shall** be submitted and validated separately prior to submission;

1785 **Note 1:** An ESV may not be required, if the entropy is collected outside the sub-chip
1786 cryptographic subsystem, depending on changes to the entropy source or the
1787 subsystem housing it. Please refer to [IG 9.3.A](#) and [IG D.J](#) for details on applicable
1788 caveats and entropy estimates.

1789 **Note 2:** Single chip embodiments may implement an ESV or a DRBG linked to a dedicated
1790 entropy source inside the physical boundary. Such cases may be implemented (a)
1791 inside the sub-chip cryptographic subsystem or (b) in two or more sub-chip
1792 cryptographic subsystems. The case (b) represents multiple disjoint sub-chip
1793 cryptographic subsystems (see Resolution 3 of [IG 2.3.B](#)).

- 1794
1795
1796
1797
- c. Approved security functions **shall** be retested and validated by the CAVP if implemented in a soft circuitry core recompiled in a different part configuration. In Web Cryptik, this case may be captured as a checkbox under the PTSC submission scenario (e.g., the CSTL selects “CAVP Testing Redone”).

- 1798 **Note 3:** If the original algorithm testing was performed as stated in the [Management Manual](#)
 1799 Section 7.3 – *Testing using Emulators and Simulators* in a module simulator, and there is
 1800 no change to the soft-core, no additional algorithm testing is required.
- 1801 d. Full regression testing (see FIPS 140-3 [Resources page](#)) **shall** be performed on the new
 1802 sub-chip cryptographic subsystem after fabrication (transformation of the HDL to a gate
 1803 or physical circuitry representation);
- 1804 e. **ISO/IEC 19790:2012** Section 7.3 **shall** be addressed for the new single-chip module for
 1805 all Security Levels within this Section.
- 1806 f. **ISO/IEC 19790:2012** Section 7.7 **shall** be addressed for the new single-chip module at
 1807 Security Level 1.
- 1808 g. **ISO/IEC 19790:2012** Sections 7.11.2 and 7.11.9 **shall** be addressed for the new single-
 1809 chip module for all Security Levels within this Section.
- 1810 h. A new Security Policy **shall** be provided for the new single-chip module.
- 1811 i. Versioning information on the new certificate **shall** be provided for:
- 1812 o the new physical single-chip,
 1813 o non-security relevant single-chip functional subsystem firmware if applicable,
 1814 o the sub-chip cryptographic subsystem soft and hard circuitry cores (which are
 1815 unchanged from the original validation), and
 1816 o the associated firmware.
- 1817 j. The only time code changes are allowed as part of an PTSC is if they are non-security
 1818 relevant and *necessary* to correctly run the module on the new/modified single chip
 1819 environment (e.g., compilation flags or configuration options that need to be updated).
 1820 No other changes are permitted (even to incorporate other non-security relevant changes
 1821 such as bug fixes). In Web Cryptik, this may be captured as a checkbox under the PTSC
 1822 submission scenario (e.g., the CSTL selects “Limited NSRL”).

1823 7.1.10 Update (UPDT)

1824 Modifications are made to hardware, software or firmware components **that affect some of the**
 1825 **FIPS 140-3 security relevant items**. Per [IG 2.4.A](#), “the term *security* is not defined in the Terms
 1826 and Definitions, but, within the scope of FIPS 140-3, is determined based on the Section 6
 1827 Functional Security Objectives, and the specific Section 7 Security Requirements derived from
 1828 those objectives”. An updated cryptographic module can be considered in this scenario if less
 1829 than a 30% of security changes were made to the module. Security changes include impacts to:
 1830 approved / allowed security functions/algorithms, SSPs, approved security services, self-tests,
 1831 and security states within the FSM. None of these, assessed individually, can exceed 30% of
 1832 changes. The individual ratios for each of these **shall** be provided to the CMVP within the
 1833 Revalidation Change Document (e.g., 2 changes to approved security services out of 10 total
 1834 results in 20% change).

1835 The CSTL is responsible for identifying the documentation that is needed to determine whether a
 1836 revalidation is sufficient, and the vendor is responsible for submitting the requested
 1837 documentation to the CSTL. Documentation may include a previous validation report and
 1838 applicable CMVP rulings, design documentation, source code, source code difference evidence,
 1839 FSM etc.

1840 The CSTL **shall**:

- 1841 a. provide a summary of the changes and rationale of why this meets the <30% guideline.
 1842 The CMVP upon review, may determine that the changes are >30% and **shall** be
 1843 submitted as an FS.
- 1844 b. review and independently verify the accuracy of the vendor-supplied documentation and
 1845 identify any additional documentation necessary to confirm the applicability of this
 1846 revalidation scenario.
- 1847 c. identify the assertions affected by the modification and **shall** perform the tests associated
 1848 with those assertions. This will require the CSTL to:
- 1849 i. Review the COMPLETE list of assertions applicable to the module,
 - 1850 ii. Identify, from the previous validation report, the assertions that have been
 1851 affected by the modification,
 - 1852 iii. Identify additional assertions that were NOT previously tested but should now be
 1853 tested due to the modification, and
 - 1854 iv. Review assertions where specific Implementation Guidance (IG) was provided to
 1855 confirm that the module meets all current applicable IGs.

1856 In addition to the tests performed against the affected assertions, the CSTL **shall** perform the
 1857 regression test suite shown on the [CMVP website](#).

1858 The UPDT can also be used to for resetting the module's sunset date when a module has not
 1859 changed, provided the above requirements are met.

1860 UPDT can be combined with any submission scenario(s). In Web Cryptik, there may be an
 1861 option for the CSTL to select the appropriate checkbox(s) after choosing the UPDT submission
 1862 scenario.

1863 7.1.11 Common Vulnerabilities and Exposures (CVE)

1864 A CSTL has been contracted to perform a revalidation for a module on which the vendor has
 1865 made FIPS 140 security-relevant changes in response to one or more CVEs (Common
 1866 Vulnerability and Exposure). For more information about CVEs please see <https://cve.mitre.org/>.

1867 This revalidation scenario provides the vendor with a means to quickly fix, test, and revalidate a
 1868 module subject to a *security-relevant CVE*¹ while at the same time providing assurance that the
 1869 module still meets the FIPS 140-3 standard. If a CVE does not require security-relevant changes
 1870 to address it, then the vendor may pursue an NSRL revalidation.

1871 To complete a Scenario CVE revalidation:

- 1872 a. The CSTL **shall** determine that security relevant changes to the module are only
 1873 to correct the vulnerability disclosed in the CVE. Other changes are permitted if
 1874 only directly impacted by the CVE change (e.g., addressing the CVE may require
 1875 changing the version number, and that requires the show version service be
 1876 updated). In WebCryptik, this may be captured by selecting "Limited NSRL"
 1877 checkbox after choosing the CVE submission scenario.
- 1878 b. The CSTL **shall** examine each modification and confirm that the change does not
 1879 conflict with the requirements of FIPS 140-3.

- 1880 c. The CSTL **shall** determine that no other modifications have been made.
- 1881 d. The CSTL **shall** identify the assertions affected by the security-relevant
- 1882 modification and **shall** perform the tests associated with those assertions.
- 1883 e. The vendor is not required to address IGs that have been published since
- 1884 submission of the original module, besides following the continual guidance of [IG](#)
- 1885 [11.A](#) (CVE Management).
- 1886 f. If the fix to address the CVE is in the scope of an algorithm implementation (e.g.,
- 1887 involves a change that requires retesting per the CAVP), then this algorithm **shall**
- 1888 be CAVP tested again to obtain a new CAVP certificate with the new module
- 1889 version. In this case, the CSTL selects the “CAVP Testing Redone” sub-option in
- 1890 Web Cryptik after choosing the CVE submission scenario.

1891 In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the

1892 predefined regression tests shown on the [CMVP website](#), under CVE.

1893 Because the change to the module is to address a security-relevant CVE, **the previous version of**

1894 **the module is no longer considered validated (in essence, Revoked) and shall be removed**

1895 **from the certificate**; exceptions may be made if the vendor shows how the CVE can be

1896 mitigated by policies included in the Security Policy, while still adhering to the FIPS 140-3

1897 standard.

1898 ¹ A *security-relevant CVE* is one that affects how the module meets the Section 6 Functional

1899 Security Objectives, and the specific Section 7 Security Requirements derived from those

1900 objectives.

1901 7.1.12 Algorithm Transition (TRNS)

1902 A CSTL has been contracted to perform a revalidation for a module on which the vendor has

1903 made FIPS 140-3 security relevant changes solely in response to a published CMVP algorithm

1904 transition that will cause some previously validated modules to be placed on the Historical list

1905 (see [Programmatic Transitions](#) webpage for a list of such algorithms). For example, the 2024

1906 non-SP 800-56Brev2 RSA-based key encapsulation/un-encapsulation transition explained in

1907 FIPS 140-3 [IG D.G](#). If the algorithm transition will NOT cause the module to move to the

1908 historical list (i.e., considered a “soft” transition), changes cannot be made as part of this

1909 submission.

1910 Note: a single Scenario TRNS submission may combine multiple algorithm transitions.

1911 However, this may increase review time.

1912 The purpose of the TRNS revalidation is to provide the vendor a means to quickly address

1913 algorithm transition requirements, test and revalidate a module in order to meet a CMVP

1914 transition, while at the same time providing assurance that the module still meets the FIPS 140-3

1915 standard.

1916 If the module code is *changed* to address an algorithm transition, the following requirements

1917 apply:

- 1918 a. Submitted as a Scenario TRNS.

- 1919 b. The CSTL **shall** determine that security relevant changes to the module are only
 1920 to address a specific CMVP transition. Other changes are permitted if only
 1921 directly impacted by the TRNS change (e.g., addressing the TRNS may require
 1922 changing the version number, and that requires the show version service be
 1923 updated). In Web Cryptik, this may be captured as a checkbox under the TRNS
 1924 submission scenario (e.g., the CSTL selects “Limited NSRL”).
- 1925 c. The CSTL **shall** examine each modification and confirm that the change does not
 1926 conflict with the requirements of FIPS 140-3.
- 1927 d. The CSTL **shall** determine that no other modifications have been made. The
 1928 vendor is not required to address IGs or guidance that have been published since
 1929 submission of the original module, unless directly applicable to the transitioning
 1930 algorithm (e.g., CAVP testing or self-test requirements).
- 1931 e. The CSTL **shall** identify the assertions affected by the security-relevant
 1932 modification and **shall** perform the tests associated with those assertions.
- 1933 f. If the means to meet the transition are in the scope of an algorithm
 1934 implementation, and the path chosen to meet the requirements necessitates testing,
 1935 then this algorithm **shall** be CAVP tested to obtain a new CAVP certificate with
 1936 the new module version. In Web Cryptik, this may be captured as a checkbox
 1937 under the TRNS submission scenario (e.g., the CSTL selects “CAVP Testing
 1938 Redone”).
- 1939 g. In addition to the tests performed against the affected assertions, the CSTL **shall**
 1940 also perform the predefined regression tests shown on the [CMVP website](#) under
 1941 “TRNS – Code Change” on all versions listed on the module’s certificate and on
 1942 at least one of the listed OEs for hybrid or software/firmware modules (if the
 1943 module binary image is identical across all OEs; if not, testing on at least every
 1944 binary image is required).
- 1945 h. The CSTL **shall** provide justification on why regression testing is not necessary
 1946 for the untested OEs. With proper justification, these may remain on the
 1947 module’s certificate.
- 1948 i. If regression testing is not performed on some versions, then those **shall** be
 1949 removed from the module’s certificate. OEs without proper justification or
 1950 regression testing **shall** be removed from the module’s certificate.

1951 If the module code is *unchanged* to address an algorithm transition and the change is purely to
 1952 documentation, one of the following four options apply. For each option, the CSTL **shall** state
 1953 that the change to address the transition is purely documentary and which option applies.

1954 **Option 1:** services or functionality were not moved to or from an approved mode to remain
 1955 compliant (e.g., services remain in an approved mode but are updated to demonstrate compliance
 1956 to the applicable algorithm standard rather than moved into a non-approved mode), then the
 1957 vendor may pursue a Scenario [ALG](#) revalidation.

- 1958 **Option 2:** The vendor moves all non-compliant functionality into a non-approved mode of
 1959 operation from an approved mode of operation.
- 1960 a. Submitted as a Scenario TRNS.
- 1961 b. The CSTL **shall** determine that security relevant changes to the module are only
 1962 to address a specific CMVP transition.
- 1963 c. The CSTL **shall** examine each modification and confirm that the change does not
 1964 conflict with the requirements of FIPS 140-3.
- 1965 d. The CSTL **shall** determine that no other modifications have been made. The
 1966 vendor is not required to address IGs or guidance that have been published since
 1967 submission of the original module, unless directly applicable to the transitioning
 1968 algorithm (e.g., CAVP testing or self-test requirements).
- 1969 e. The CSTL **shall** identify the assertions affected by the security-relevant
 1970 documentation modification and **shall** perform the tests associated with those
 1971 assertions.
- 1972 f. The CSTL **shall** demonstrate how the module still meets [IG 2.4.C](#) after the
 1973 reclassification of non-compliant functionality into a non-approved mode of
 1974 operation. Due to this FIPS 140-3 requirement that all approved security services
 1975 have an unambiguous indicator (AS02.24), **it does not seem likely/possible that**
 1976 **a FIPS 140-3 validation fall under this Option 2**, where code is unchanged yet
 1977 a previously approved service is moved to the non-approved mode, as that would
 1978 surely invalidate the approved indicator for this service.
- 1979 g. In addition to the tests performed against the affected assertions, the CSTL **shall**
 1980 also perform the predefined regression tests shown on the [CMVP website](#) under
 1981 “TRNS - No Code Change” on all versions listed on the module’s certificate and
 1982 on at least one of the listed OEs for hybrid or software/firmware modules (if the
 1983 module binary image is identical across all OEs; if not, testing on at least every
 1984 binary image is required).
- 1985 The only exception to this requirement (g.) is if the algorithm being transitioned is
 1986 part of a standalone service and is not used by any other module service (e.g.,
 1987 cryptographic library where the module only provides the algorithm as an API
 1988 service to a calling application as a stand-alone service). In this case, the CSTL
 1989 **shall** provide justification on why regression testing is not necessary at all.
- 1990 j. The CSTL **shall** provide justification on why regression testing is not necessary
 1991 for the untested OEs. With proper justification, these may remain on the
 1992 module’s certificate.
- 1993 k. If regression testing is not performed on some versions, then those **shall** be
 1994 removed from the module’s certificate. OEs without proper justification or
 1995 regression testing **shall** be removed from the module’s certificate.

- 1996 h. The CSTL **shall** provide assurance that the non-compliant functionality is not
 1997 used to meet any FIPS 140-3 requirements (key/CSP establishment, generation,
 1998 storage, etc.).
- 1999 i. The CSTL **shall** provide assurance, upon module examination, that no service,
 2000 algorithm or CSP that relied on or used the non-compliant functionality,
 2001 parameters, keys, etc. remain in an approved mode. An approved mode **shall**
 2002 only contain approved services.
- 2003 j. Documentation **shall** be updated to indicate the module does not utilize non-
 2004 compliant functionality in an approved mode of operation.

2005 **Option 3:** The vendor recategorizes the non-compliant functionality as claiming no security per
 2006 [IG 2.4.A](#), and this functionality remains in an approved mode of operation.

- 2007 a. The same rules for Option 2 above **shall** be followed except for bullets ‘i’ and ‘j’.
- 2008 b. The CSTL **shall** provide justification on how the requirements of [IG 2.4.A](#) are
 2009 met. This scenario is intended to be rarely used/accepted and depends on the
 2010 purpose or use of the service that utilizes the non-approved algorithms. For
 2011 example, a software library implementing three-key Triple-DES Encryption as
 2012 one of its approved services cannot simply state this algorithm does not claim any
 2013 security (per [IG 2.4.A](#)) and be used in an approved mode, as this does not meet 3)
 2014 or 4) in [IG 2.4.A](#) Additional Comment #2.

2015 **Option 4:** A combination of any of three options above (ALG, moving non-compliant
 2016 functionality into the a non-approved mode, and/or recategorized per [IG 2.4.A](#)), in which case,
 2017 requirements of each option apply.

- 2018 a. Submitted as a Scenario TRNS.
- 2019 b. Each option **shall** be listed/indicated in the Revalidation Change Document under
 2020 Option 4 (e.g. under Option 4, the following are claimed: Options 1 and 2) and
 2021 note how each of the applicable ‘shall’ statements for each option are met).

2022 In order to accommodate vendors who are updating their validation to prepare for an algorithm
 2023 transition, fully compliant TRNS or ALG revalidations that have addressed the transition and are
 2024 submitted to the CMVP before the date the transition is to take effect, will remain on the active
 2025 list through the completion of the revalidation, even if it is not completed until after the transition
 2026 date, unless the algorithm transition is to address a security concern that is deemed unacceptable
 2027 by the CMVP. For newly submitted ALG submissions that address the transition, the CSTL
 2028 **shall** include in the Special Instructions field the text “algorithm_ transition” (with or without the
 2029 underscore) in order for the CMVP not to move this submission to the historical list come the
 2030 algorithm transition date.

2031 Changes made to a module in order to meet a transition are security-relevant, whether to the
 2032 module code or purely to documentation, due to their potential impacts on core and downstream
 2033 services and the treatment of keys and SSPs. For example, moving *allowed* functionality from
 2034 an approved mode to a non-approved mode - by either changing the software/firmware or a
 2035 purely documentation change - is considered security relevant. Therefore, besides the case in

2036 **Option 1** above, all submissions that address a transition will require a Scenario UPDT, TRNS
2037 or FS submission regardless of module type or security level.

2038 If a Scenario TRNS revalidation addresses an algorithm transition that moved the original
2039 certificate to the Historical list, and the sunset date of the certificate has yet to expire, then upon
2040 the revalidation of the module under Scenario TRNS, a new certificate will be issued on the
2041 Active list (inheriting the original sunset date) for the version of the module compliant with the
2042 transition requirements. Otherwise, if the original certificate was moved to the Historical list for
2043 reasons that are not addressed in the TRNS revalidation (e.g., a separate algorithm transition or
2044 the sunset date expired), the new certificate will be shown on the Historical list *immediately* after
2045 completion of the TRNS revalidation.

2046 7.1.13 Physical Enclosure (PHYS)

2047 Modifications are made only **to the physical enclosure of the cryptographic module that**
2048 **provides its protection and involves no operational changes to the module.** The CSTL is
2049 responsible for ensuring that the change only affects the physical enclosure (integrity) and has no
2050 operational impact on the module. The CSTL **shall** fully test the physical security features of the
2051 new enclosure to ensure its compliance to the applicable requirements of the standard.

2052 The CSTL **shall**:

- 2053 a. Describe the change (pictures may be required),
- 2054 b. State that it is a security relevant change,
- 2055 c. Provide sufficient information supporting that the physical only change has no
2056 operational impact,
- 2057 d. Describe the tests performed by the CSTL that confirm that the modified enclosure still
2058 provides the same physical protection attributes as the previously validated module. For
2059 physical security levels 2, 3 and 4, the CSTL **shall** submit an updated Physical Security
2060 Test Report.

2061 7.1.14 Submission Scenario Summary Table

Scenario	Active or Historical ¹	New or Updated Cert ²	New Sunset Date ³	Meet All Latest Guidance ⁴	Code changes ¹⁰	CAVP ¹¹	ESV ⁵	ENT Remain on Cert ⁷	Pre-defined Regression Testing ⁸	Submission Process ⁹
VUP	A or H	Updated	No	No	No	No	No	Possible	No (nor optional testing)	Email
VAOE	A or H	Updated	No	No	No	No	No	Possible	No (nor optional testing)	Email
NSRL	A only	Updated	No	No	Limited	No	No	Possible	No	Email
ALG	A only	Updated	No	No (except for the updated algorithm)	No	Yes (updated alg)	No	Possible	No	Email
OEUP	A only	Updated	No	No	Limited	Yes (new OEs)	Yes ⁶	Possible	Yes (full regression table)	Email
RBND	A only	New	No	No	Limited	No	No	Possible	No (nor optional testing)	Email
PTSC	A only	New	No	No	Limited	Yes (new OEs)	Yes ⁶	Possible	Yes (full regression table)	Email
UPDT	A or H	New	Yes	Yes	< 30 %	Yes	Yes	No	Yes (full regression table)	Web Cryptik
CVE	A or H	Updated	No	No	Limited	Possible	No	Possible	Yes (subset of regression table)	Email
TRNS	A or H	New	No	No (except for the algorithm transitioning)	Limited	Possible	No	Possible	Yes (subset of regression table)	Email
PHYS	A only	Updated	No	No	No	No	No	Possible	Yes (physical security)	Email
FS	N/A	New	Yes	Yes	N/A	Yes	Yes	No	Full testing	Web Cryptik

2062 ¹ A or H means the revalidation can be on a completed validation that is either Active *or* Historical; A
 2063 only means it can only be on an Active validation.

2064 ² The result of this validation or revalidation will either be a new certificate (new number) or an updated

2065 certificate (same number).

2066 ³ The result of this validation or revalidation will either be a new sunset date of 5 years, or the sunset date
2067 will remain the same. See Additional Comment #3 below for more details.

2068 ⁴ If Yes, the validation or revalidation **shall** meet all the latest applicable guidance and requirements (e.g.,
2069 standards, implementation guidance, management manual guidance, algorithm testing/self-tests, and other
2070 CMVP guidance) at the time of submission to the CMVP unless there is an implementation guidance
2071 transition that affects reports in the queue. If No, the revalidation **shall** meet all applicable requirements
2072 at the time of *original* validation (a module does not need to meet requirements that were added since the
2073 time of original validation, except those specified in the table).

2074 ⁵ Is ESV testing required (if applicable per [IG 9.3.A](#))?

2075 ⁶ Only required on the new OEs for OEUP, or new single-chip environments for PTSC.

2076 ⁷ Only for the original validation's ENT claim. No new ENT claims are possible, for any validation or
2077 revalidation.

2078 ⁸ Note: additional regression testing (on top of the predefined ones) may be applicable per requirements of
2079 the scenario. See the [CMVP FIPS 140-3 Resources](#) page for the pre-defined regression tests.

2080 ⁹ The CMVP has emailed the CSTLs with additional revalidation scenario guidance that details the
2081 temporary submission processes as these scenarios are being incorporated into Web Cryptik.

2082 ¹⁰ Are code changes permitted?

2083 ¹¹ Is CAVP testing required?

2084 7.1.15 Additional Comments

2085 1. If the individual section(s) security level is being lowered as part of the revalidation,
2086 this is considered security relevant and the module may be submitted as a UPDT with
2087 full testing on the individual section(s) that is being lowered or impacted by the
2088 change.

2089 2. If the individual section(s) security level is being raised or if the physical embodiment
2090 changes, e.g., from multi-chip standalone to multi-chip embedded, then the
2091 cryptographic module will be considered a new module and **shall** undergo full
2092 validation testing by a CSTL and submitted as an FS.

2093 3. The sunset date for the module is determined based on the scenario:

2094 • Scenarios FS, UPDT – sunset date will be 2 years (interim validation) or 5 years
2095 (full validation) from the date the module was validated

2096 • Scenarios VUP, VAOE, NSRL, ALG, OEUP, CVE, PHYS – sunset date unchanged

2097 • Scenarios RBND, PTSC, TRNS – sunset date is inherited from the original
2098 certificate

2099 4. It is **not** possible to combine any revalidation scenarios outside of what is explicitly
2100 permitted by the submission scenario. For example, if a vendor would like to rebrand
2101 (RBND) a PTSC submission, this would need to happen in two separate submissions (i.e.,

2102 RBND followed by a PTSC). Similarly, despite it being a simple change, a VUP or VAOE
 2103 would need to be submitted separately and cannot be combined with other scenarios
 2104 (besides FS and UPDT). This will give the CMVP the most flexibility to address each
 2105 scenario submission effectively and efficiently.

2106 A summary table of the permitted combinations are below:

		Secondary scenario											
		VUP	VAOE	NSRL	ALG	OEUP	RBND	PTSC	UPDT	CVE	TRNS	PHYS	
Main Submission	VUP	-	-	-	-	-	-	-	-	-	-	-	-
	VAOE	-	-	-	-	-	-	-	-	-	-	-	-
	NSRL	-	-	-	-	-	-	-	-	-	-	-	-
	ALG	-	-	-	-	-	-	-	-	-	-	-	-
	OEUP	-	-	✓	x	-	-	-	-	-	-	-	-
	RBND	x	-	✓	✓	-	-	-	-	-	-	-	✓
	PTSC	-	-	✓	✓	-	-	-	-	-	-	-	-
	UPDT	-	-	x	✓	✓	✓	✓	✓	-	✓	✓	✓
	CVE	-	-	✓	✓	-	-	-	-	-	-	-	-
	TRNS	-	-	✓	✓	-	-	-	-	-	-	-	-
	PHYS	-	-	-	-	-	-	-	-	-	-	-	-

2107 x - The secondary scenario will NOT be separately selectable as a sub-option in WebCryptik
 2108 (e.g., VUP changes are always part of a RBND).

2109 ✓ - The secondary scenario WILL be separately selectable as a sub-option but will likely be
 2110 further locked down / limited per the Main Submission scenario guidance (e.g., NSRL changes
 2111 associated with an OEUP submission must be specific to running the new OEs, rather than
 2112 permitting *any* NSRL changes).

2114 For the revalidation scenarios that *can* be combined (i.e., checkbox in the table above), the
 2115 main submission **shall** meet all applicable requirements of the secondary scenario, in
 2116 addition to the main scenario requirements, and document both scenarios in the Change
 2117 Document. For example, a RBND + NSRL must document and include all NSRL
 2118 regression testing as applicable.

2119 5. A revalidation submission cannot be performed on a submission that is in the queue. It
 2120 **shall** be on a completed validation (e.g., UPDT on a *validated* FS). However, see sections
 2121 4.4.5 (*Resubmission while in Review Pending*) and 4.4.6 (*Changes while in Coordination*)
 2122 for permitted changes while in the queue within the same submission.

2123 7.2 CMVP requirements pertaining to testing and approved algorithms

2124 FIPS 140-3 describes approved security functions which can be used in an approved mode of
 2125 operation, and non-approved security functions which cannot be used in an approved mode of
 2126 operation. Approved security functions are expected to be CAVP tested, but CAVP testing may
 2127 rarely not yet be available for these methods.

2128 In such cases where CAVP testing is not available, guidance must be written to permit using
 2129 these algorithms in an approved mode. These algorithms may be “vendor affirmed” to meet the
 2130 applicable standard(s).

2131 In addition, security methods that fall outside of the list of approved methods cannot be used in
 2132 an approved mode, unless guidance is written to permit such special cases, where these methods
 2133 are *allowed* to be used in the approved mode of operation; or as permitted under AS02.21.

2134 The next two sections explain when vendor affirmed or *allowed* methods are permitted, as well
 2135 as the transitioning from vendor affirmed to CAVP Testing.

2136 7.2.1 Vendor Affirmation of Security Functions and Methods

2137 If CAVP testing is not available or the module is submitted during a transition period, then the
 2138 following guidance is applicable.

2139 If new approved methods (e.g., NIST FIPS, SP, etc.) are added to SP 800-140 documents, until
 2140 such time that CAVP testing is available or the transition period has not yet expired for the new
 2141 method, the CMVP may:

- 2142 ○ permit vendor affirmation of the new approved method if supported by existing IG(s)
 2143 (untested, listed as approved for use in an approved mode with the caveat “vendor
 2144 affirmed”). If no such IG is published, vendor affirmation is not possible.

2145 Notes:

- 2146 1. The Cryptographic Technology Group (CTG) at NIST may determine prior methods may be
 2147 retroactively disallowed and moved to non-approved and not permitted in an approved mode
 2148 of operation (e.g., DES). A transition notice would appear in NIST publications.
- 2149 2. For all approved methods, all applicable FIPS 140-3 requirements must be met.
- 2150 3. The CMVP may decide to *allow* methods in the approved mode that are non-approved with
 2151 supported by existing IG(s) (untested, and listed as non-approved but *allowed* in an approved
 2152 mode; e.g., see IGs [D.F](#) and [D.G](#)).
- 2153 4. **Vendor Affirmed:** a security method reference that is listed with this caveat has not been
 2154 tested by the CAVP, and the CMVP or CAVP provide no assurance regarding its correct
 2155 implementation or operation. Only the vendor of the module affirms that the method or
 2156 algorithm was implemented correctly.
- 2157 5. The users of cryptographic modules implementing vendor affirmed security functions must
 2158 consider the risks associated with the use of untested and unvalidated security functions.

2159 7.2.2 Transitioning from vendor affirmed to CAVP Testing

2160 When CAVP algorithm testing is released on the ACVTS production server in any of the
 2161 following 3-month periods identified below, the transition occurs at the end of the following 3-
 2162 month transition date. More specifically:

CAVP testing release	CMVP report submitted by
Jan 1 – March 31	June 30
April 1 – June 30	Sept 30
July 1 – Sept 30	Dec 31
Oct 1 – Dec 31	March 31

2163 *Table 1 - CAVP testing release dates and subsequent CMVP Transition dates*

2164 To illustrate, if the CAVP releases new testing for algorithm A, B and C, during the July 1 –
 2165 September 30 period, then the transition date will be September 30 + three months, so after
 2166 December 31 vendor affirming to algorithms A, B, or C will be prohibited in initial report
 2167 submissions.

2168 During the transition period, a new approved method would either be listed as approved with a
 2169 reference to a CAVP validation certificate, or as vendor affirmed if testing was not performed
 2170 and an IG that supports vendor affirmation of this algorithm was met.

2171 When the transition period ends, for newly received test reports:

- 2172 ○ only approved methods that have been tested, receives a CAVP validation certificate
 2173 and is verified to meet the underlying algorithm standard is permitted. All other
 2174 methods would be listed as non-approved and not allowed in an approved mode of
 2175 operation.
- 2176 ○ the vendor could optionally follow up with testing of untested vendor affirmed methods
 2177 and if so, the reference to vendor affirmed would be removed and replaced by reference
 2178 to the algorithm certificate. If there are no changes to the module, this change can be
 2179 submitted under Scenario ALG (see Section 7.1 – *Submission Scenarios*). If the
 2180 module is changed, this can be submitted under Scenarios UPDT or FS as applicable.

2181 **Note:** To track the algorithms and their transition dates, the CMVP maintains a table available on
 2182 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions)
 2183 [transitions](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions)).

2184 **Note:** If a self-test requirement is associated with the algorithm, the algorithm will only be
 2185 considered as an approved algorithm by CMVP if the self-test requirement is also met.

2186 7.3 Testing using Emulators and Simulators

2187 Under certain circumstances it may not be possible to test a module or algorithm directly. In
 2188 these cases, CMVP has permitted the use of emulators and simulators to model the behavior of
 2189 the item being tested. It is important to note the differences of these models and to apply them
 2190 under the correct circumstances.

2191 An emulator attempts to “model” or “mimic” the behavior of a cryptographic module. The
 2192 correctness of the emulators' behavior is dependent on the inputs to the emulator and how the
 2193 emulator was designed. It is not guaranteed that the actual behavior of the cryptographic module
 2194 is identical, as other variables may not be modeled correctly or with certainty.

2195 A simulator exercises the actual source code (e.g., Very High-Speed Integrated Circuit (VHSIC)
 2196 Hardware Description Language (VHDL) code) prior to physical entry into the module (e.g., a
 2197 Field-Programmable Gate Array (FPGA) or custom Application-Specific Integrated Circuit
 2198 (ASIC)). From a behavioral perspective, the behavior of the source code within the simulator
 2199 may be logically identical when placed into the module or instantiated into logic gates. However,
 2200 many other variables exist that may alter the actual behavior (e.g., path delays, transformation
 2201 errors, noise, environmental, etc.). It is not guaranteed that the actual behavior of the
 2202 cryptographic module is identical, as many other variables may not be identified with certainty.

2203 Labs may apply emulators or simulators depending on the type of testing results to be achieved.
 2204 There are three broad areas of focus during the testing of a cryptographic module: operational
 2205 testing of the module at the defined boundary of the module, algorithm testing and operational
 2206 fault induction testing.

- 2207 1. Operational Testing – Emulation or simulation is prohibited for the operational testing of a
 2208 cryptographic module. Actual testing of the cryptographic module must be performed
 2209 utilizing the defined ports and interfaces and services that a module provides. A test
 2210 harness or a modified version to induce an error may be utilized; however, no changes to
 2211 code or circuitry responsible for the tested response may be made.
- 2212 2. Operational Fault Induction – An emulator or simulator may be utilized for fault induction
 2213 to test a cryptographic module’s transition to error states as a complement to the source
 2214 code review. Rationale must be provided for the applicable TE as to why a method does
 2215 not exist to induce the actual module into the error state for testing.
- 2216 3. Algorithm Testing – Algorithm testing utilizing the defined ports and interfaces and
 2217 services that a module provides is the preferred method. This method most clearly meets
 2218 the requirements of [IG 2.3.A](#). If this preferred method is not possible where the module’s
 2219 defined set of ports and interfaces and services do not allow access to internal algorithmic
 2220 engines, two alternative methods may be utilized:
 - 2221 a. A module may be modified under the supervision of the CSTL for testing purposes
 2222 to allow access to the algorithmic engines (e.g., test jig, test API), or
 - 2223 b. A module simulator may be utilized.

2224 When submitting the algorithm test results to the CAVP, the actual OE on which the
 2225 testing was performed must be specified (e.g., including modified module identification or
 2226 simulation environment). When submitting the module test report to the CMVP, AS2.20
 2227 must include rationale explaining why the algorithm testing was not conducted on the

2228 actual cryptographic module. An emulator may not be used for algorithm testing.

2229 **7.4 Remote Testing of Modules**

2230 The guidance below addresses the need for testing a module remotely while obtaining the
 2231 equivalent assurance as if the test were performed at the **vendor's facility**. All physical security
 2232 testing except for Environment failure protection/testing (i.e., EFT/EPT tests: TE.07.73.01,
 2233 TE.07.77.01-03 and TE.07.81.01-02) **shall** be performed in person by a CSTL tester at either the
 2234 vendor site, the CSTL site and/or remote site as per HB 150-17 requirements.

2235 The CSTL may perform some or all testing remotely. If the testing is performed remotely at the
 2236 vendor site, the following conditions **shall** be met:

- 2237 1. a. The hardware, firmware or hybrid IUT is located at the vendor site.
- 2238 b. The software IUT is located at the vendor site or 3rd party cloud system.
- 2239 2. The vendor remotely provides a cryptographic module to the test laboratory and its
 2240 boundary and version are verified against the Security Policy. (ISO/IEC 24759
 2241 TE04.13.01, 02, 03). The module boundary and version **shall** be verified at the beginning
 2242 of any new remote testing sessions.
- 2243 3. a. The network access and/or video conference to a remote test operational environment,
 2244 in support of actual testing, **shall** be authorized and controlled by the vendor.
- 2245 b. A 3rd party cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google
 2246 Cloud) may be used as a service in support of module validation (e.g. video conference
 2247 and data storage) if:
 - 2248 • all HB 150-17 and NVLAP General Criteria Checklist ISO_IEC 17025
 2249 requirements are met; and
 - 2250 • the remote testing requirements are met.
- 2251 c. A 3rd party cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google
 2252 Cloud) may be used as a testing platform if:
 - 2253 • all HB 150-17 and NVLAP General Criteria Checklist ISO_IEC 17025
 2254 requirements are met;
 - 2255 • the remote testing requirements are met;
 - 2256 • the environment provides the same level or additional level of security as
 2257 the lab would provide for internal testing;
 - 2258 • the cryptographic module under test **shall** be confirmed to be running on
 2259 an OE that is well-defined and has a specific OS version, hardware
 2260 platform and version, and processor (including microprocessor version) as
 2261 shown on the module's certificate and security policy; and

- 2262 • the OS version, hardware platform and version, and processor **shall** be
2263 confirmed during the testing session.
- 2264 d. As permitted within a signed agreement by the lab and vendor:
- 2265 • The tester’s network **shall** be connected to the vendor’s network via a
2266 secure connection (e.g., VPN or SSH) ; and/or
- 2267 • A secure video conference **shall** be used and the recording done in a
2268 secure manner.
- 2269 e. The tester’s tools must satisfy the lab’s network requirements before connecting to the
2270 vendor’s network to test the module if applicable.
- 2271 4. The CSTL **shall** have a procedure for conducting remote testing at the vendor site which
2272 includes the following:
- 2273 a. All the remote testing sessions that produce the final test results **shall** be recorded and
2274 archived at the CSTL as evidence material to demonstrate the tester control and/or
2275 oversight (as per bullet 6 below) (e.g. video conference records and/or detailed test plan)
2276 and to capture the test results (e.g. video conference records, screenshots and/or log files).
- 2277 b. If multiple remote testing sessions are required, a log which includes the date and the
2278 test being conducted **shall** be maintained and archived.
- 2279 c. If during testing, the IUT version or subversion (e.g. pre-release, debug) changes, the
2280 final test report being submitted **shall** reflect the final version of the IUT.
- 2281 d. If there are multiple simultaneous testing activities occurring at the vendor site, a
2282 system of separation between the different cryptographic module test activities **shall** be
2283 maintained.
- 2284 e. For all conformance testing and validations, the CSTL **shall** ensure that any file
2285 containing iterative, not final, test results are isolated from the final test results.
- 2286 f. It is the CSTL’s responsibility to ensure that any version iteration during the testing
2287 doesn’t impact any of the final results transmitted to the CMVP.
- 2288 5. The required operational environment information (e.g., operating system name and
2289 version, processor family, hardware platform model) **shall** be obtained and verified
2290 against the operational environment information listed on the CAVP algorithm certificates
2291 for this module.
- 2292 6. The tester is accountable and therefore **shall** understand, oversee, direct, and/or assume
2293 control of testing operations to initialize, install, and operate the module. The tester is
2294 accountable to ensure the proper initialization, installation and operation of the module
2295 through the entire testing at the CSTL site and/or vendor site for the multiple testing
2296 sessions as applicable.
- 2297 7. If a test harness is used, it **shall** be reviewed or written by the lab. It **shall** be verified to
2298 have been maintained properly with no vendor manipulation prior to its execution. The

2299 test results on the remote operational environment **shall** be captured and transmitted back
 2300 to lab without the risk of being modified. The tester **shall** verify the test harness runs
 2301 properly on its operational environment. The tester must verify the integrity of the testing
 2302 session as well as the completeness and accuracy of the test results.

2303 8. The remote testing **shall** cover the same set of FIPS 140-3 requirements including but not
 2304 limited to the following list, as if the operational environment were local to the tester:

2305 a. The services listed in the module Security Policy can be invoked or directed/overseen
 2306 and verified by the tester.

2307 b. For a module to be validated at Level 2 or 3 for ISO/IEC 19790:2012 Section 7.4.4,
 2308 the role-based or identity-based authentication **shall** be performed or
 2309 directed/overseen and verified by the tester.

2310 c. The failure of self-tests and the subsequent transition to an error state where module
 2311 data output interfaces are inhibited can be observed and verified by the tester.

2312 d. As applicable per IG 9.3.A, entropy has been effectively analyzed and received an
 2313 ESV for all specific OEs and/or platforms prior to submission.

2314 The vendor must provide a signed affirmation letter to the lab describing the remote testing
 2315 process and access control mechanism that allows the lab to perform the test on the remote
 2316 operational environment and protects the integrity of the test results. The lab **shall** provide a
 2317 signed letter to the CMVP stating that the module had been tested remotely, affirming that the
 2318 vendor provided their affirmation letter, stating what TEs were tested remotely, and explaining
 2319 how the requirements were met during the remote testing.

2320 It is the CSTL's responsibility to ensure that the assurance level is maintained when remote
 2321 testing is being conducted.

2322 Additional Comments:

2323 1. It is the responsibility of the tester to determine if a module is eligible to be tested remotely. If
 2324 the tester cannot demonstrate a test requirement during remote testing, then the module **shall** not
 2325 be fully tested remotely. If the tester wishes to test a subset of test requirements remotely, the
 2326 remaining test requirements **shall** be tested onsite at the CSTL site or in person by the CVP tester
 2327 at the vendor site.

2328 2. The tester **shall** confirm that the operational environment exactly matches the agreed upon test
 2329 environment, including any virtual environments used. A Virtual Machine may not be used in
 2330 lieu of an OS, unless the VM has been agreed to be part of the test environment and will be listed
 2331 on the certificate.

2332 3. A record of the testing location, related documentation (e.g. equipment proof of calibration)
 2333 and CSTL tester(s) who conducted the testing **shall** be maintained. This is applicable for all
 2334 tests including physical security testing.

2335 4. The above vendor site remote testing requirements are also applicable to 3rd party remote site
 2336 in addition to existing the HB 150-17 and NVLAP General Criteria Checklist ISO_IEC 17025
 2337 requirements.

2338 5. Regardless of the location of the testing, it is the CSTL's responsibility to ensure that all HB
 2339 150-17 and NVLAP General Criteria Checklist ISO_IEC 17025 requirements are met (e.g.
 2340 NVLAP General Criteria Checklist ISO_IEC 17025: **6.4.2**, **6.4.3**, 6.4.6, 6.4.7, 6.4.8, **7.1.4**
 2341 requirements; and HB 150-17 B.2.2 & B.3 requirements).

2342 6. Regarding any ITAR related questions, please refer to [https://www.ecfr.gov/current/title-](https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.54)
 2343 [22/chapter-I/subchapter-M/part-120/subpart-C/section-120.54](https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.54).

2344 **7.5 Partial validations and non-applicable areas**

2345 CMVP will not issue a validation certificate unless the cryptographic module meets at least the
 2346 Security Level 1 requirements for each area in Section 6 of ISO/IEC 24759:2017. Areas can be
 2347 designated as Not Applicable (N/A) if they meet the following criteria:

- 2348 • Section 6.5, Software/Firmware Security may be designated as N/A if the module is
 2349 hardware-only without firmware (or software);
- 2350 • Section 6.6, Operational Environment may be designated as N/A if the operational
 2351 environment for the cryptographic module is a limited or non-modifiable operational
 2352 environment and Section 6.7, Physical Security is greater than Security Level 1
 2353 (AS06.04).
- 2354 • Section 6.7, Physical Security may be designated as N/A if the cryptographic module is a
 2355 software-only module and thus has no physical protection mechanisms;
- 2356 • Section 6.8, Non-invasive security is N/A by default as there are currently no
 2357 requirements in SP 800-140F. Any claims for non-invasive will be identified under
 2358 Section 6.12.
- 2359 • Section 6.12, Mitigation of Other Attacks is Applicable if the module has been purposely
 2360 designed, built, and publicly documented to mitigate one or more specific attacks (see [IG](#)
 2361 [12.A](#)). Otherwise, this section may be designated as N/A.

2362 **7.6 CMVP requirements for PIV validations**

2363 PIV card applications can only be tested on a CMVP validated module, such as a smartcard. The
 2364 CMVP validated module then obtains NPIVP validation, by adding the PIV card application to
 2365 the module. The validated smartcard and the PIV card application is then re-validated as a
 2366 CMVP module.

2367 A PIV card application that is included as a component of a cryptographic module **shall** be
 2368 referenced on the module validation. The cryptographic module validation entry **shall** provide
 2369 reference to the PIV card application(s) validation certificate number. The cryptographic
 2370 module's versioning information **shall** include the complete versioning information of the
 2371 module including the PIV application(s). Each PIV application's name **shall** be clearly

2372 identified, and the PIV Certificate number is referenced on the CMVP module validation.

2373 The PIV NPIVP validation entry includes the following information:

- 2374 1. the name of the PIV card application,
- 2375 2. the name of the cryptographic module the PIV application was tested on, and
- 2376 3. the complete versioning information of the module including the PIV application(s)

2377 The NPIVP validation entries can be found at:

2378 [https://csrc.nist.gov/projects/nist-personal-identity-verification-program/validation-lists/piv-card-](https://csrc.nist.gov/projects/nist-personal-identity-verification-program/validation-lists/piv-card-application-validation-list)
 2379 [application-validation-list](https://csrc.nist.gov/projects/nist-personal-identity-verification-program/validation-lists/piv-card-application-validation-list)

2380 7.7 Module count definition

2381 Moved to the following CMVP webpage (under “MIS Field Descriptions”):

2382 <https://csrc.nist.gov/projects/cmvp/sp800-140b>

2383 7.8 Module definitions for same certificates

2384 To be on the same certificate, each module version **shall** have identical:

- 2385 1. Section and overall levels.
- 2386 2. Suite of approved security services.
- 2387 3. Cryptography.
- 2388 4. Suite of security functions and underlying algorithms, modes, and key sizes.
- 2389 5. Suite of SSPs associated with the security services.
- 2390 6. Suite of roles and authentication methods.
- 2391 7. Finite State Model except related to the allowed differences.
- 2392 8. SSP establishment methods.
- 2393 9. Self-tests.
- 2394 10. Design assurance.
- 2395 11. Mitigation of other attacks.
- 2396 12. Module type (i.e., Software, Hardware, Firmware, or Hybrid).
- 2397 13. Module embodiments (i.e., single-chip, multi-chip embedded/standalone) with similar
- 2398 physical construction including physical boundary.

2399 7.9 Vendor or User Affirmation of Modules

2400 The tested/validated module version, OE upon which it was tested, and the originating vendor
 2401 are stated on the validation certificate entry. The certificate validation entry serves as the
 2402 benchmark for the module-compliant configuration. This guidance addresses two separate
 2403 scenarios: changes a **Vendor** (7.9.1) can affirm the module will perform as tested in the CSTL’s
 2404 validation submission and changes a **User** (7.9.2) can affirm the module will perform as tested in
 2405 the CSTL’s validation submission.

2406 This guidance is *not applicable* for validated modules when the requirements of **ISO/IEC**

2407 **19790:2012** Section 7.7 Physical Security has been validated at Levels 2 or higher. This
 2408 guidance is however, applicable at Physical Security Level 1 for *firmware* or *hybrid* modules.

2409 7.9.1 Vendor

2410 1. A vendor may perform post-validation recompilations of a software, firmware, or hybrid
 2411 module and affirm the modules continued validation compliance. By adding vendor support
 2412 of non-tested configurations to the validated module security policy, the vendor bears all
 2413 responsibility. These non-tested configurations versions may be considered by the user at
 2414 their risk, provided the following is maintained:

2415 a) Software modules do not require any source code modifications (e.g., changes, additions,
 2416 or deletions of code) to be recompiled and ported to another OE and must:

2417 i) For **Level 1 OE**, a software cryptographic module can be considered compliant with
 2418 the FIPS 140-3 validation when operating on any general-purpose platform/processor
 2419 that supports the specified operating system as listed on the validation entry or
 2420 another compatible⁴ operating system, or

2421 ii) For **Level 2 OE**, a software cryptographic module can be considered compliant with
 2422 the FIPS 140-3 validation when operating on any general-purpose platform/processor
 2423 that supports the same level 2 operational environment settings specified on the
 2424 validation entry.

2425 b) Firmware modules do not require any source code modifications (e.g., changes, additions,
 2426 or deletions of code) to be recompiled, and its identified unchanged tested operating
 2427 system (i.e., same version or revision number) may be ported together from one platform
 2428 to another platform while maintaining the module's validation.

2429 Level 2 and above Firmware modules cannot be ported and maintain their validation,
 2430 since Physical Security must be retested.

2431 c) Hybrid modules may be ported together from one OE to another OE while maintaining
 2432 the module's validation provided that they do not require any of the following:

2433 i) software or firmware source code modifications (e.g., changes, additions, or deletions
 2434 of code) to be recompiled and its identified unchanged tested operating system (i.e.,
 2435 same version or revision number) or another compatible operating system;

2436 ii) modified hardware components utilized by the software or firmware (e.g., changes,
 2437 additions, or deletions).

2438 Level 2 and above hybrid modules cannot be ported and maintain their validation, since
 2439 Physical Security must be retested.

2440 The CMVP allows vendor porting and re-compilation of a validated software, firmware or
 2441 hybrid cryptographic module from the OE specified on the validation certificate to an OE
 2442 which was not included as part of the validation testing as long as the porting rules are

⁴ Compatibility may be based on how the module is compiled (e.g., for a specific processor, or general purpose). General purpose (universal) can be ported to other OEs. OSs of the same "family" could be another example of compatibility.

2443 followed. Vendors may affirm that the module works correctly in the new OE. However, the
 2444 CMVP makes no statement as to the correct operation of the module or the security strengths
 2445 of the generated keys when so ported if the specific OE is not listed on the validation
 2446 certificate.

2447 The vendor **shall** work with a CSTL to update the security policy and submit it to the CMVP
 2448 under one of the available revalidation scenarios (see submission scenario [VAOE](#) in Section
 2449 7.1). The update would affirm and include references to the new vendor affirmed OE(s) (see
 2450 related table in SP 800-140B and SP 800-140Brev1). The module's Security Policy **shall**
 2451 include a statement that no claim can be made as to the correct operation of the module or the
 2452 security strengths of the generated keys when ported to an OE which is not listed on the
 2453 validation certificate.

2454 2. Software or firmware modules that require source code modifications (e.g., changes,
 2455 additions, or deletions of code) to be recompiled and ported to another hardware or OE must
 2456 be reviewed by a CSTL and revalidated per [Section 7.1](#) (including regression testing) to
 2457 ensure that the module does not contain any OE-specific or hardware environment-specific
 2458 code dependencies. See Scenarios UPDT, NSRL, and OEUP. This is not porting or vendor
 2459 affirming the OE but rather incorporating the new versions and environment onto the
 2460 certificate.
 2461

2462 The vendor must meet all applicable requirements in ISO/IEC 19790:2012 Section 7.11 Life-
 2463 cycle assurance, SP 800-140 Section 6.11 Life-cycle assurance and related CMVP IGs.

2464 7.9.2 User

2465 **A user may not modify a validated module. Any user modifications invalidate a module**
 2466 **validation.**⁵

2467 A user may perform post-validation porting of a module and affirm the module's continued
 2468 validation compliance provided the following is maintained:

2469 1. For **Level 1 OE**, a software, firmware, or hybrid cryptographic module will remain
 2470 compliant with the FIPS 140-3 validation on any general-purpose platform/processor that
 2471 supports the specified operating system listed on the validation entry, or another compatible
 2472 operating system.

2473 The user may affirm that the module works correctly in the new OE if the porting rules are
 2474 followed. However, the CMVP makes no statement as to the correct operation of the module or
 2475 the security strengths of the generated keys when ported and executed in an OE not listed on the
 2476 validation certificate.

⁵ A user may post-validation recompile a module if the unmodified source code is available and the module's Security Policy provides specific guidance on acceptable recompilation methods to be followed as a specific exception to this guidance. The methods in the Security Policy must be followed without modification to comply with this guidance.

2477 **7.10 Operational Equivalency Testing for HW Modules**

2478 CMVP requires full testing of any module that the vendor wishes to list on the certificate.
 2479 However, modules may be grouped together if they are the same except for devices listed under
 2480 Equivalence Categories, which are currently considered for five classes of devices. Each
 2481 Category and sample technologies for each Category are provided in Table 2.

Category	Examples
Memory/Storage Devices	<ul style="list-style-type: none"> ○ HDD, SSD, DRAM, NAND, NOR, ROM, Solid State Memory Device, USB Flash Drive ○ Optical Disk Drive ○ Magnetic Tape Drive
Field Replaceable and Stationary Accessories	<ul style="list-style-type: none"> ○ Power Supplies ○ Fans
Interfaces (I/O Ports)	<ul style="list-style-type: none"> ○ Port Count ○ Line Card Count ○ Serial: RS232, RS422, RS485 ○ SAS, SATA, eSATA ○ Fiber Optic, FCoE, Fiber Channel ○ Ethernet, FireWire, DVI, SCSI, USB
Computational Devices	Refer to CAVP equivalency criteria and entropy constraints for guidance
Programmable Logic Devices	<ul style="list-style-type: none"> ○ CPLD, FPGA, PAL

2482 *Table 2 - Equivalence Categories*

2483 For details on the Equivalency Categories, please see the Equivalency Categories Tables under
 2484 the [FIPS 140-3 Resources Tab](#) of the CMVP website. Also note, for modules that have
 2485 differences within each of those categories, the level of testing required is dependent on the
 2486 differences. Some differences require analysis only, while others require full or limited
 2487 regression testing. The following are the general categories of the levels of testing. The actual
 2488 testing required depends on the Equivalency Category (See Equivalency Regression Test Table
 2489 and Equivalency Categories Tables found under the [FIPS 140-3 Resources Tab](#) of the CMVP
 2490 website):

- 2491 - Analysis Only (AO) for Equivalency Category X: Once the equivalency evidence/argument

2492 is provided and validated for the Equivalency Category X, there is no additional test other
 2493 than the proof of its physical existence required on a module with the equivalent components
 2494 in Category X to the module that has been fully tested under the same validation.

2495 - Required Testing (RT) for Equivalency Category X:

2496 o If a module has some security relevant differences in the Equivalency Category X, the
 2497 module **shall** be tested against all of the listed TEs for that category in Equivalency
 2498 Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP website.

2499 o If a module claims equivalency in multiple categories in comparison to a fully tested
 2500 module under the same validation, all of the required TEs for each claim equivalency
 2501 category **shall** be satisfied.

2502 - Focused Testing (FT) for Equivalency Category X:

2503 o The use of some technologies may introduce Security Relevant differences that cannot be
 2504 predicted by this Section 7.10. For example, Programmable Logic Devices may be used
 2505 to support the Cryptographic Module in a number of different ways that are security
 2506 relevant (e.g., authentication). It is up to the lab to determine what section of the standard
 2507 is affected by this security relevant difference and apply the Revalidation Regression Test
 2508 Table found under the FIPS 140-3 Resources Tab of the CMVP website. For other
 2509 sections not affected by this difference, Regression Testing per Equivalency Regression
 2510 Test Table found under the FIPS 140-3 Resources Tab of the CMVP website shall be
 2511 performed.

2512 - Complete Regression Testing (CRT): If an equivalency justification cannot be made, or the
 2513 module differences can be mapped to a CRT entry within Equivalency Categories Tables
 2514 under the FIPS 140-3 Resources Tab of the CMVP website, all modules, which lack an
 2515 equivalency justification must, according to their security level, satisfy each TE listed in the
 2516 Revalidation Regression Test Table under the FIPS 140-3 Resources Tab of the CMVP
 2517 website.

2518 In each report where the vendor wishes to claim equivalency, the lab **shall**:

2519 - List the Equivalency Category, and specific component types being claimed in TE02.15.01.
 2520 The lab must justify the component categorizations. The assumption is that the vendor
 2521 initiated the Equivalency Category argument while the lab performed the analysis.

2522 - List the additional testing performed (if any) between the modules. This list **shall** be
 2523 provided as an addendum to the test report.

2524 - Include in the Test Report how each module meets the TE's that are required for testing per
 2525 this Section 7.10.

2526 For example:

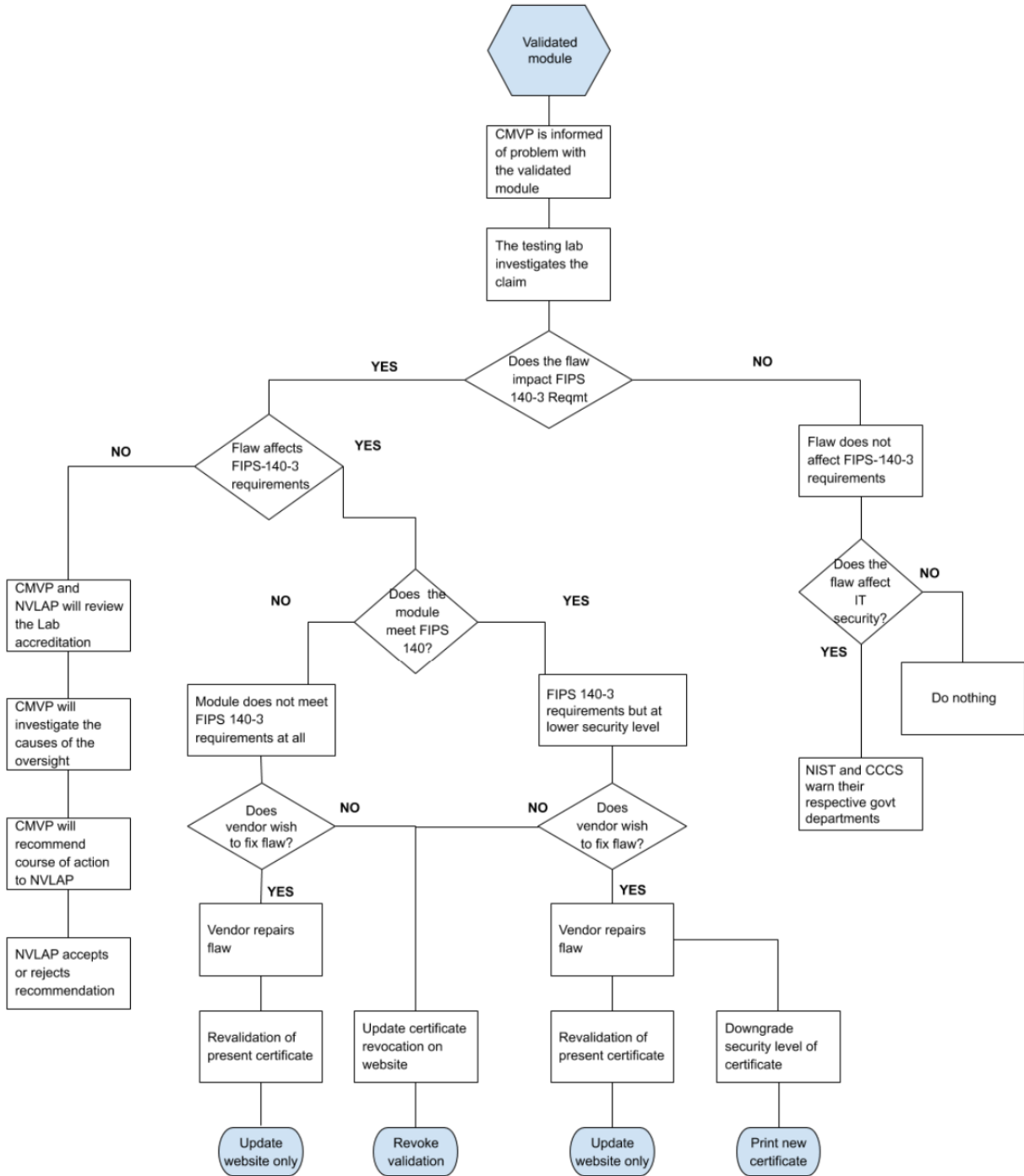
2527 - Two devices to be on the same certificate have Hard Drives with different storage capacities,
 2528 so testing requirement is Analysis Only, e.g., proof that both modules exist as claimed by the
 2529 vendor.

2530 - Two devices to be on the same certificate have different types of Solid State Memory: one
 2531 has NOR Flash and the other has NAND. This will require a small selection of testing, per

- 2532 Equivalency Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP
2533 website.
- 2534 - Two devices to be on the same certificate have different types of storage: one has a Hard
2535 Disk and the other has a Solid-State Drive. This will require complete regression testing per
2536 Revalidation Regression Test Table.
- 2537 Additional Comments
- 2538 - The lab **shall** perform full testing on at least one module.
- 2539 - This only applies to Operational testing of Hardware modules
- 2540 - Physical security testing (ISO/IEC 19790:2012, section 7.7) is not addressed for Security
2541 Level 2 and above. In other words, this does not exempt the lab from performing physical
2542 security testing for modules at Level 2 or above. This is because the lab needs to examine
2543 each module for, e.g., opacity and tamper evidence, if there are physical differences between
2544 the modules.
- 2545 - Components considered equivalent may still affect the entropy generated within the modules
2546 in different ways. This must be accounted for in the ESV report, if ESV is applicable.
- 2547 - Equivalency considerations of the main processors/CPU's are out of scope of this Section
2548 7.10. If the CPU is different between modules on the same certificate, then the full
2549 Revalidation Regression Test Table must be run (found under the FIPS 140-3 Resources Tab
2550 of the CMVP website).
- 2551 - ISO/IEC 24759:2017 Section 6.7 Physical Security, Section 6.8 Non-Invasive Security and
2552 Section 6.12 Mitigation of Other Attacks are out of scope of this guidance.
- 2553

2554 **Annex A CMVP Post Validation Issue Assessment Process**

2555 **Annex A.1 Addressing Security Relevant Issues**



2556

2557 *Figure 5- Annex A. Validation Issue Assessment Process*

2558 **Annex A.2 Addressing CVE Relevant Vulnerabilities**

2559 The list of CVEs is maintained by NIST in the NVD at <https://nvd.nist.gov/>. The purpose of the
2560 Scenario CVE revalidation (described in Section 7.1) is to provide the vendor a means to quickly
2561 fix, test and revalidate a module that is subject to a security-relevant CVE, while at the same
2562 time providing assurance that the module still meets the current FIPS 140 standards.

2563 Vendors must reference this database and address the security relevant CVE's that are within the
2564 boundary of the module, not only during the validation process, but also after the module has
2565 been validated. Without published security relevant CVEs being addressed by the vendor and
2566 verified by the testing laboratory, the CMVP has no assurance that the module meets the
2567 requirements to obtain or maintain validation.

2568 At the discretion of the CMVP, certificates will be revoked that do not comply. It is the goal of
2569 the CMVP to maintain the security of validated modules.

2570 For more information about CVEs please also refer to <https://cve.mitre.org/>. See also [IG 11.A](#)
2571 [CVE Management](#) for more guidance on this topic.

2572 **ACRONYMS**

2573	ACVTS	Automated Cryptographic Validation Testing System
2574	ANSI	American National Standards Institute
2575	AS	Assertion
2576	CAVP	Cryptographic Algorithm Validation Program
2577	CCCS	Canadian Centre for Cyber Security
2578	CMVP	Cryptographic Module Validation Program
2579	CMUF	Cryptographic Module User Forum
2580	CR	Cost Recovery
2581	CSTL	Cryptographic and Security Testing Laboratory
2582	CVC	Consolidated Validation Certificate
2583	CVE	Common Vulnerabilities and Exposures
2584	CVP	Cryptographic Validation Program
2585	DES	Data Encryption Standard
2586	ECR	Extended Cost Recovery
2587	ESV	Entropy Source Validation
2588	FIPS	Federal Information Processing Standard
2589	FISMA	Federal Information Security Management Act
2590	FSM	Finite State Model
2591	GC	Government of Canada
2592	HB	Handbook
2593	ID	Identification
2594	IG	Implementation Guidance
2595	ISO	International Organization for Standardization
2596	ITAR	International Traffic in Arms Regulation
2597	IUT	Implementation Under Test
2598	N/A	Not Applicable
2599	NIST	National Institute of Standards and Technology
2600	NVLAP	National Voluntary Laboratory Accreditation Program
2601	OE	Operational Environment
2602	OS	Operating System
2603	PDF	Portable Document Format

2604	RFG	Request for Guidance
2605	SP	Special Publication
2606	TE	Tester Evidence
2607	TID	Tracking Identification Number
2608	TR	Test Requirements
2609	URL	Uniform Resource Locator
2610	VE	Vendor Evidence