

FIPS 140-3
Cryptographic Module Validation Program
Management Manual

(Date 12/06/2023)

Version 2.0

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.

Table of Contents

Contents

1	INTRODUCTION	6
1.1	Background	6
1.2	Purpose of the CMVP Management Manual	6
1.3	Applicability and Scope	6
1.4	Purpose of the CMVP	6
1.5	Purpose of the Cryptographic Algorithm Validation Program (CAVP)	7
1.6	Use of Validated Products	7
1.7	CMVP Management Manual Structure	7
1.8	CMVP Related Documents	8
1.8.1	FIPS 140-3	8
1.8.2	Security Requirements for Cryptographic Modules	8
1.8.3	Test requirements for cryptographic modules	9
1.8.4	NIST SP 800-140x	9
1.8.5	Implementation Guidance	10
1.8.6	Web Cryptik User Guide	10
1.8.7	CSTL Accreditation Standards	10
1.8.8	Additional information on the CMVP Website	11
2	CMVP MANAGEMENT	13
2.1	Introduction	13
2.2	Validation Authority	13
2.3	Programmatic Directives, Policies, Internal Guidance and Documentation	13
2.4	CMVP Points of Contact	13
2.4.1	Language of Correspondence	13
2.5	Request for Guidance from CMVP	13
2.5.1	Request for Guidance Details	14
2.5.2	Request for Guidance Format	15
2.5.3	Post Validation Inquiries	16
2.6	Roles and Responsibilities of Program Participants	17
2.6.1	Vendor	17
2.6.2	Cryptographic and Security Testing Laboratory	17
2.6.3	CMVP Validation Authorities	18
2.6.4	Validated Module User	19

2.7	CMVP Meetings	19
2.7.1	CSTL Manager Meetings	19
2.7.2	CMUF participation	20
2.8	Confidentiality of Information	20
3	CSTL PROCESSES	22
3.1	Accreditation of CMVP scopes for CSTLs	22
3.1.1	Accreditation Process for the CMVP scope	22
3.2	Maintenance of CSTL Accreditation	26
3.2.1	Proficiency of CSTL	26
3.2.2	Renewal of Accreditation	27
3.2.3	Ownership of a CSTL	27
3.2.4	Relocation of a CSTL	27
3.2.5	Change of Approved Signatories	27
3.2.6	Change of Key Laboratory Testing Staff	28
3.2.7	Monitoring Visits	28
3.2.8	Suspension, Denial and Revocation of Accreditation	28
3.2.9	Voluntary Termination of the CSTL	29
3.3	Confidentiality of Proprietary Information	29
3.3.1	Confidentiality of Proprietary Information Exchanged between NIST, CCCS and the CSTL	29
3.3.2	Non-Disclosure Agreement for Current and Former Employees	30
3.4	Code of Ethics for CSTLs	30
3.5	Management of CMVP and CAVP Test Tools	30
4	CMVP PROCESSES	31
4.1	Cryptographic Module Validation Process Overview	31
4.1.1	Vendor, CSTL, and CMVP duties for Testing of the Cryptographic Module	31
4.2	Implementation Under Test (IUT) and Modules in Process (MIP)	34
4.3	Submission Scenarios	34
4.4	Validation Submission Queue Processing	34
4.4.1	Full and Update Submission Validations	34
4.4.2	All other submissions	35
4.4.3	HOLD Status for Cryptographic Modules on the Modules In Process	35
4.4.4	Validation Deadline	36
4.4.5	Resubmission while in Review Pending	36
4.4.6	Changes during Coordination	37
4.5	Validation when Test Reports are not Reviewed by both Validation Authorities	37
4.5.1	Controlled Unclassified Information	38
4.6	CMVP Fees	39
4.6.1	Cost Recovery Fee	39
4.6.2	Extended Cost Recovery Fee	39
4.6.3	NIST Payment Policy	40

4.6.4	Invoice for a Report Submission	40
4.6.5	Request for Transition Period Extension	41
4.7	Flaw Discovery Handling Process	41
4.8	Validation Revocation	42
4.9	Entropy Source Validation (ESV) Processes	42
4.9.1	Entropy Source Validation Submissions	42
4.9.1.1	Entropy Source Validation WebClient	44
4.9.1.2	Entropy Source Validation Python Client	44
4.9.2	Entropy Source Validation Comment Remediation Process	44
4.9.3	Entropy Source Validation Webpages	44
4.10	CMVP Webpages	45
4.10.1	Official CMVP Website	45
4.10.2	Cryptographic Module Validation Lists	45
4.10.3	CMVP Certificate Page Links	46
4.10.3.1	Security Policy	46
4.10.3.2	Consolidated Validation Certificate	46
4.10.3.3	Vendor Link	47
4.10.3.4	Vendor Product Link	47
4.10.3.5	Algorithm Certificates	47
4.10.3.6	Validation History	47
4.10.3.7	Usage of FIPS 140-3 Logos	47
5	CMVP AND CAVP PROGRAMMATIC METRICS COLLECTION	48
5.1	Overview	48
5.2	Confidentiality of the Collected Metrics Data	48
5.3	Collected Metrics	48
6	TEST TOOLS	49
6.1	Web Cryptik	49
6.2	Suggested Tools for Physical Testing	49
7	CMVP GENERAL TESTING AND REPORTING GUIDANCE	51
7.1	Submission Scenarios	51
7.1.1	Requirements for all submissions	51
7.1.2	Full Submission (FS)	52
7.1.3	Vendor Update (VUP)	52
7.1.4	Vendor Affirmed Operational Environment (VAOE)	53
7.1.5	Non-Security Relevant (NSRL)	53
7.1.6	Algorithm Update (ALG)	54
7.1.7	Operational Environment Update (OEUP)	54
7.1.8	Rebrand (RBND)	55
7.1.9	Port Sub Chip (PTSC)	56
7.1.10	Update (UPDT)	57
7.1.11	Common Vulnerabilities and Exposures (CVE)	58
7.1.12	Algorithm Transition (TRNS)	59

7.1.13	Physical Enclosure (PHYS)	62
7.1.14	Submission Scenario Summary Table	63
7.1.15	Additional Comments	64
7.2	CMVP requirements pertaining to testing and approved algorithms	65
7.2.1	Vendor Affirmation of Security Functions and Methods	66
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	69
7.5	Partial validations and non-applicable areas	72
7.6	CMVP requirements for PIV validations	72
7.7	Module count definition	73
7.8	Module definitions for same certificates	73
7.9	Vendor or User Affirmation of Modules	73
7.9.1	Vendor	74
7.9.2	User	75
7.10	Operational Equivalency Testing for HW Modules	75

List of Figures

Figure 1 - Roles, Responsibilities, and Output in the CMVP Process.....	17
Figure 2 - CSTL NVLAP scopes	22
Figure 3 - CSTL Accreditation Process	23
Figure 4- Cryptographic Module Testing and Validation Process	31
Figure 5- Annex A. Validation Issue Assessment Process	79

List of Tables

Table 1 - CAVP testing release dates and subsequent CMVP Transition dates.....	67
Table 2 - Equivalence Categories	76

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 guidance for the
19 management of the CMVP as authorized by FIPS 140-3, and the conduct of activities necessary
20 to ensure that the standards, as referenced in FIPS 140-3, are fully met.

21 1.3 Applicability and Scope

22 The *CMVP Management Manual* is applicable to the CMVP Validation Authority, the CSTLs,
23 and the vendors who participate in the program. Consumers who procure validated cryptographic
24 modules may also be interested in the contents of this manual. This manual outlines the
25 management activities and specific responsibilities which have been assigned to the various
26 participating groups. This manual does not deal with the actual standards and technical aspects of
27 the standards.

28 1.4 Purpose of the CMVP

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

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

36 finding value in the use of validated cryptography.

37 CMVP Validation is performed through conformance testing to requirements for cryptographic
38 modules as specified in FIPS 140. Accredited third-party CSTLs perform independent assurance
39 testing with CMVP oversight. CMVP is the Validation Authority, a joint initiative between the
40 Government of Canada and the Government of the United States of America. For more
41 information about CMVP see: [https://csrc.nist.gov/projects/cryptographic-module-validation-](https://csrc.nist.gov/projects/cryptographic-module-validation-program)
42 [program](https://csrc.nist.gov/projects/cryptographic-module-validation-program).

43 **1.5 Purpose of the Cryptographic Algorithm Validation Program (CAVP)**

44 The purpose of the CAVP is to increase assurance of cryptographic algorithms through a testing
45 process. Validation is achieved by testing the algorithm and comparing results to known or
46 expected answers. Tests are to demonstrate compliance with cryptographic standards listed in SP
47 800-140C, SP 800-140D, and SP 800-140E. More information about CAVP can be found at:
48 <https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program>.

49 **1.6 Use of Validated Products**

50 Both public and private sectors can use cryptographic modules validated to FIPS 140 for the
51 protection of sensitive information. As specified under FISMA of 2002, U.S. Federal
52 departments and agencies are required to use cryptographic modules validated to FIPS 140 for
53 the protection of sensitive information where cryptography is required. Similarly, the CCCS
54 recommends that GC departments and agencies use those validated cryptographic modules for
55 the protection of Protected information.

56 **1.7 CMVP Management Manual Structure**

57 This manual is organized into the following sections:

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

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

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

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

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

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

68 **Section 7 – CMVP General Testing and Reporting Guidance** adds requirements to
69 manage the CMVP testing program, minimizing retest and maximizing testing
70 flexibility while maintaining assurance.

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

73 **1.8 CMVP Related Documents**

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

81 1.8.1 FIPS 140-3

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

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

93 1.8.2 Security Requirements for Cryptographic Modules

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

104 The standard is typically reviewed by an ISO committee every three years for consideration of
105 revision. Copies can be obtained from ISO.org. NIST made available a limited number of copies
106 of ISO/IEC 19790:2012. To request a copy of ISO/IEC 19790:2012 and ISO/IEC 24759:2017
107 (see below), see the CMVP webpage, [https://csrc.nist.gov/Projects/cryptographic-module-
108 validation-program/fips-140-3-standards](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards).

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

111 1.8.3 Test requirements for cryptographic modules

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

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

128 1.8.4 NIST SP 800-140x

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

133 **NIST SP 800-140** specifies the Test Requirements (TR) for Federal Information Processing
134 Standard (FIPS) 140-3. SP 800-140 modifies the TE and/or VE requirements of ISO/IEC
135 24759:2017. As a validation authority, the CMVP may modify, add, or delete TEs and/or VEs as
136 specified under section 5.2 of ISO/IEC 24759:2017. This NIST SP should be used in conjunction
137 with ISO/IEC 24759:2017 as it modifies only those requirements identified in this document.

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

143 **NIST SP 800-140B** is to be used in conjunction with ISO/IEC 19790:2012 Annex B and
144 ISO/IEC 24759:2017 6.14. The SP modifies only those requirements identified in this document.
145 SP 800-140B also specifies the content of the tabular and graphical information required in
146 ISO/IEC 19790:2012 Annex B. As a validation authority, the CMVP may modify, add, or delete
147 VE and/or TE specified under paragraph 6.14 of ISO/IEC 24759:2017 and as specified in
148 ISO/IEC 19790:2012 paragraph B.1.

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

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

156 **NIST SP 800-140E** replaces the approved authentication mechanism requirements of ISO/IEC
 157 19790:2012 Annex E. As a validation authority, the CMVP may supersede this Annex in its
 158 entirety with its own list of approved authentication mechanisms. This document supersedes
 159 ISO/IEC 19790:2012 Annex E and ISO/IEC 24759:2017 paragraph 6.17.

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

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

165 1.8.5 Implementation Guidance

166 *Implementation Guidance* is issued to provide clarification and guidance with respect to an
 167 assertion or group of assertions found in the documents listed above. Often, implementation
 168 guidance is issued to assist CSTLs and vendors to apply the requirements to a particular type of
 169 cryptographic module implementation or technology. Implementation guidance is also issued
 170 based on responses by NIST and CCCS to questions posed by the CSTLs, vendors, and other
 171 interested parties. The document is available on-line on the official website at
 172 <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/announcements>.

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

174 1.8.6 Web Cryptik User Guide

175 This guide is available in the Help area of the Web Cryptik tool. It covers the use of FIPS 140-3
 176 Web Cryptik. It is expected to be updated often as new functionality, edits, and program changes
 177 are introduced. The user guide may also identify where IG information requested should be
 178 included in the report and security policy. This guide also provides guidance on how to fill in the
 179 available fields (e.g., vendor name, Hardware/Software/Firmware versioning, algorithms,
 180 caveats, and operational environment).

181 **Responsible Position:** CMVP Technology Manager.

182 1.8.7 CSTL Accreditation Standards

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

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

186 NIST Handbook 150 (2020), *NVLAP Procedures and General Requirements*,
187 NIST Handbook 150-17 (2022), *NVLAP Cryptographic and Security Testing*,
188 Document

189 Links for these documents are available at [https://www.nist.gov/nvlap/publications-and-](https://www.nist.gov/nvlap/publications-and-forms/nvlap-handbooks-and-lab-bulletins)
190 [forms/nvlap-handbooks-and-lab-bulletins](https://www.nist.gov/nvlap/publications-and-forms/nvlap-handbooks-and-lab-bulletins).

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

192 1.8.8 Additional information on the CMVP Website

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

- 194 1. Announcements ([https://csrc.nist.gov/Projects/Cryptographic-Module-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Announcements)
195 [Validation-Program/Announcements](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Announcements)) contains information on changes made to
196 documents or test tools.
- 197 2. Notices ([https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Notices)
198 [Program/Notices](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Notices)) contains copies of statements published in the Federal Register,
199 programmatic or policy updates or information not related to CMVP documents or
200 test tools.
- 201 3. Validated Modules ([https://csrc.nist.gov/Projects/Cryptographic-Module-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules)
202 [Validation-Program/Validated-Modules](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules)) contains the link to the search tool for
203 finding a specific module, or aspects of a module validation. In addition, the page
204 contains information describing categories (active, historical, and revoked) and
205 explains the difference between a module that is a product vs one that is a component.
- 206 4. Implementation Under Test (IUT) List
207 ([https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List)
208 [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
209 cryptographic modules undergoing testing. The result of the testing has not yet been
210 submitted to the CMVP. Inclusion of a module on this list is voluntary, dependent on
211 the vendor. The CMVP has no information regarding the status of these modules and
212 does not know if or when a test report will be submitted to the CMVP. The modules
213 are listed by vendor name. For more information regarding a specific module, please
214 contact the vendor.
- 215 5. 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)
216 [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
217 review status for each cryptographic module whose scenario type is FS (Full
218 submission) or UPDT (Update). The list tracks the test report after it has been
219 submitted to the CMVP through validation. For each submission, the status and the
220 date it went into that state is listed. The date will also be updated for any new
221 submission to the CMVP, even if the status remains the same. For additional
222 information regarding a specific module, please contact the vendor.
- 223 6. Programmatic Transitions ([https://csrc.nist.gov/Projects/cryptographic-module-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions)
224 [validation-program/programmatic-transitions](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions)) lists algorithm-related transitions.
225 Applicable standards, relevant IGs, ACVTS availability, and the beginning CMVP

226 acceptance date are listed for each algorithm/scheme. Also available is information
227 related to deprecated algorithms/schemes that force validated module certificates to
228 the historical category. Included in this list are deadlines for last submission date as
229 an approved algorithm/scheme as well as the date whereby the validation certificate
230 of an approved module using the algorithm/scheme will be moved to the Historical
231 list.

232 7. Management Manual ([https://csrc.nist.gov/Projects/cryptographic-module-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual)
233 [validation-program/cmvp-fips-140-3-management-manual](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual)) contains the link to the
234 latest version of this manual.

235 8. Related References ([https://csrc.nist.gov/Projects/cryptographic-module-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards)
236 [validation-program/fips-140-3-standards](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards)) describes the FIPS 140-3 standard,
237 referenced standards in FIPS 140-3, and CMVP management documents.

238 9. IG Announcements ([https://csrc.nist.gov/Projects/cryptographic-module-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements)
239 [validation-program/fips-140-3-ig-announcements](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements)) is where the latest version of the
240 FIPS 140-3 IGs can be found. The webpage also includes a short summary of
241 changes.

242 10. Resources ([https://csrc.nist.gov/Projects/cryptographic-module-validation-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/resources)
243 [program/resources](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/resources)) provides guidance that is easily bookmarked. Information that is
244 needed by vendors and CSTLs is listed here. As an example, specifically detailed
245 validation and re-validation information such as minimum testing requirements for
246 revalidation and equivalency can be found here.

247 11. SP 800-140 Series Supplemental Information
248 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-series-supplemental-information)
249 [series-supplemental-information](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-series-supplemental-information)) contains a table summarizing the SP 800-140x series
250 publications and their relationships to ISO/IEC 19790:2012(E) and ISO/IEC
251 24759:2017(E). The sub-pages of this webpage provide the supplemental information
252 associated with that SP 800-140x document.

253 12. CVP Certification Exam Information
254 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-information)
255 [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
256 individual must pass this exam.

257 13. CSTL Accreditation and Fees ([https://csrc.nist.gov/Projects/Testing-](https://csrc.nist.gov/Projects/Testing-Laboratories)
258 [Laboratories](https://csrc.nist.gov/Projects/Testing-Laboratories)) contains a link to the name and location of every CSTL accredited to
259 perform Cryptographic and Security Testing. The list also includes a point of contact
260 for each laboratory.

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

262 **2 CMVP Management**

263 **2.1 Introduction**

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

266 **2.2 Validation Authority**

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

271 **2.3 Programmatic Directives, Policies, Internal Guidance and Documentation**

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

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

279 **2.4 CMVP Points of Contact**

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

284 A list of CMVP points of contact can be found on the CMVP website at:
285 <https://csrc.nist.gov/projects/cryptographic-module-validation-program>.

286 **2.4.1 Language of Correspondence**

287 All correspondence between NIST, CCCS, NVLAP, and the CSTLs **shall** be in the English
288 language only.

289 **2.5 Request for Guidance from CMVP**

290 The CMVP suggests reviewing the CMVP Management Manual, IGs, the CMVP
291 Announcements, and CMVP Notices posted on the CMVP web sites first as answers to questions
292 may be readily available. The information found on the CMVP web site provides the official
293 position of the CMVP. If the information cannot be found in the aforementioned guidance,

294 CMVP will accept requests that are general knowledge or to a specific application. In addition,
295 CMVP will accept post-validation inquiries for any perceived issues relating to existing modules.

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

299 Once a vendor is under contract with a laboratory, NIST/CCCS will only provide official
300 guidance and clarification for the vendor's module through the point of contact at the laboratory.
301 In a situation where the vendor and laboratory are at an irresolvable impasse over a testing issue,
302 the vendor may ask for clarification/resolution directly from NIST/CCCS. The point of contact at
303 the laboratory **shall** be included on distribution of this correspondence. All correspondence from
304 NIST/CCCS to the vendor on the issue will be issued through the laboratory point of contact.

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

310 **CSTLs** must submit all test-specific questions in the Request for Guidance (RFG) format
311 described below. These questions must be submitted to all points of contact.

312 2.5.1 Request for Guidance Details

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

315 A response may require internal review by both NIST and CCCS, as well as with others as
316 necessary, and may require follow up questions from the CMVP. Therefore, such requests, while
317 time sensitive, may not be resolved immediate. If the CMVP has not sent feedback within a
318 month's time, a follow up status request is recommended.

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

322 Direct your RFG to both cmvp@nist.gov and cmvp@cyber.gc.ca. Do not send the requests to
323 individuals.

324 The email will have the subject line “[ID]-FIPS140-3-RFG-[NAME]-yyMMdd-N” where ID is
325 two-digit CSTL code (if not applicable, enter NA), NAME is the submitters name (e.g., CSTL,
326 vendor, or other entity)¹, yyMMdd is the year, month, and day of submission, and N is the
327 number of RFGs with the same subject line sent on the same day (so they are each unique).

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

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

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

331

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

335 2.5.2 Request for Guidance Format

336 For each RFG, the following information must be included, in the order outlined below:

337 **1. Clear indication of whether the RFG is PROPRIETARY or NON-PROPRIETARY**

338 *With a view to increased collaboration and transparency, if PROPRIETARY is not*
339 *indicated (preferable), the CMVP may make the RFG public in its entirety (e.g., posted*
340 *to the Cryptographic Module User Forum (CMUF)). The CMVP will remove identifiable*
341 *information if requested by the submitter.*

342 *Whether NON-PROPRIETARY or PROPRIETARY, the CMVP may derive generalized*
343 *guidance from the problem and response and share that guidance with the community*
344 *(e.g., IG or CMUF).*

345 **2. Applicable TID and/or Certificate Number**

346 *Associated TID and/or module certificate number(s). Can be N/A if unrelated to a TID*
347 *or validated module.*

348 **3. A descriptive title**

349

350 **4. A concise statement of the problem**

351

352 **5. A clear and unambiguous question regarding the problem**

353

354 **6. The configuration, embodiment of the module as it affects the answer**

355

356 **7. Applicable statement(s) from ISO/IEC 19790:2012**

357

358 **8. Applicable assertion(s), VE requirement(s), and test procedure(s) from ISO/IEC** 359 **24759:2017**

360

361 **9. Applicable assertion(s), VE requirement(s), and test procedure(s) from SP 800-140**

362

363 **10. Applicable statements from FIPS 140-3 SP800-140A, B, C, D, E, and F**

364

365 **11. Applicable statements from FIPS 140-3 Implementation Guidance**

366

367 12. Applicable statements from algorithmic standards

368

369 13. Additional background information if applicable, including any previous CMVP or
370 CAVP official rulings or guidance

371

372 14. A proposed resolution by the submitter, with justification

373

374 2.5.3 Post Validation Inquiries

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

380 An Official Request must be submitted to the CMVP in writing with signature following the
381 guidelines above. If the requestor represents an organization, the official request must be on the
382 organization's letterhead. The assertions must be objective and not subjective. The module must
383 be identified by reference to the validation certificate number(s). The specific technical details
384 must be identified and the relationship to the specific FIPS 140 Derived Test Requirements
385 assertions must be identified. The request must be non-proprietary and not prevent further
386 distribution by the CMVP.

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

392 The CSTL will state its position whether its review of the official request regarding the module:

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

396 The CMVP will review the CSTL's position and rationale supporting its conclusion. If the
397 CMVP concurs that the official request is without merit, no further action is taken. If the CMVP
398 concurs that the official request has merit, a security risk assessment will be performed regarding
399 the non-conformance issue. Please see Annex A for the flow diagram illustrating the assessment
400 process.

401 **2.6 Roles and Responsibilities of Program Participants**

402 The various roles and responsibilities of the participants in the CMVP are illustrated in Figure 1
 403 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

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

405 **2.6.1 Vendor**

406 The role of the vendor is to design and produce cryptographic modules that comply with the
 407 requirements specified in the applicable ISO/IEC standards and NIST SPs. Among other
 408 functions, the vendor defines the boundary of the cryptographic module, determines its modes of
 409 operation and its associated services, and develops an entropy and algorithm strategy and its non-
 410 proprietary security policy. When a cryptographic module is ready for testing, the vendor
 411 submits the module and the associated documentation to the accredited CSTL of its choice.

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

415 **2.6.2 Cryptographic and Security Testing Laboratory**

416 The role of the CSTL is to independently test the cryptographic module to the requirements
 417 defined for the FIPS 140-3 security level and embodiment, and to produce a written test report
 418 for the CMVP Validation Authorities based on its findings. The CSTL conducts algorithmic
 419 testing and verifies compliance to the algorithm standards (requirements may be more than what
 420 is CAVP-tested), reviews the cryptographic module’s documentation and source code, and
 421 performs requirements testing of the module in accordance with the TR, SP 800-140x and IG. If
 422 a cryptographic module conforms to all the requirements of the standards, the CSTL submits a
 423 written report to the Validation Authority. If a cryptographic module does not meet one (or
 424 more) requirements, the CSTL works with the vendor to resolve all discrepancies prior to
 425 submitting the validation package to the Validation Authority.

426 Labs **shall** confirm that claimed approved algorithms and security functions are compliant with
 427 all requirements of their respective standards (Special Publications) when some ‘shall’
 428 statements are not addressed by CAVP testing. If such compliance is not clearly demonstrated in
 429 the validation report, the CMVP may require the lab to fill in tables or answer related questions
 430 prior to validation – it is the lab’s responsibility to ensure and demonstrate full compliance for
 431 approved cryptographic claims of the module, including requirements not covered by CAVP
 432 tests.

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

- 436 1. A CSTL may not perform validation testing on a module for which the laboratory has:
 - 437 a. designed any part of the module,
 - 438 b. developed original documentation (e.g., design specifications) for any part of the
439 module,
 - 440 c. built, coded, or implemented any part of the module, or
 - 441 d. any ownership or vested interest in the module.
- 442 2. Provided that a CSTL has met the above requirements, the laboratory may perform
443 validation testing on modules produced by a company when:
 - 444 a. the laboratory has no ownership in the company,
 - 445 b. the laboratory has a completely separate management from the company, and
 - 446 c. business between the CSTL and the company is performed under contractual
447 agreements, as done with other clients.
- 448 3. A CSTL may perform consulting services to provide clarification of the *Security*
449 *requirements for cryptographic modules*, the *Test requirements for cryptographic*
450 *modules*, and other associated documents at any time during the life cycle of the module.
- 451 4. A CSTL may also create the Finite State Model (FSM), Security Policy, Entropy
452 Assessment Report (EAR) for an Entropy Source Validation, entropy Public Use
453 Document (PUD), Non-administrator guidance and Administrator guidance which are
454 specified as vendor documentation in FIPS 140-3. These must be taken from existing
455 vendor documentation for an existing cryptographic module (post-design and post-
456 development) and consolidated or reformatted from the existing information (from
457 multiple sources) into a set format. CMVP **shall** be notified of this at the time of
458 submission by providing necessary details in TEB.01.01. The CSTL must be able to show
459 a mapping from the consolidated or reformatted CSTL-created documentation back the
460 original vendor source documentation. The mapping(s) must be maintained by the CSTL
461 as part of the validation records. Source code information is considered vendor-provided
462 documentation and may be used in the CSTL-created documentation.

463 2.6.3 CMVP Validation Authorities

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

467 The role of the Validation Authorities is to establish a program to validate the testing for every
468 cryptographic module. The tests are performed, and results are documented in the submission
469 package prepared by a CSTL and reviewed by the CMVP. If the cryptographic module is
470 determined to be compliant, then the module is validated, a validation certificate is issued, and
471 the on-line validation list is updated. During the review process, the Validation Authorities

472 submit any questions they may have to the CSTL. The questions are typically technical in nature
473 and are intended to ensure that the cryptographic module meets the requirements of the standard
474 and that the information provided is accurate and complete. The CSTL may need to re-submit the
475 validation submission along with supporting documentation such as a draft validation certificate,
476 validation report, or security policy.

477 The CMVP participates, on behalf of NVLAP, in the CSTL accreditation process which
478 includes the review of the management system manual, creating and administering the
479 proficiency exam, performing the on-site assessment and the oversight of the artifact testing.

480 2.6.4 Validated Module User

481 The user verifies that a cryptographic module that they are considering procuring has been
482 validated and meets their requirements. A listing of validated cryptographic modules is
483 available from [https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-
484 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
485 each validated cryptographic module so that a potential user can determine if the validated
486 cryptographic module provides cryptographic services and protection required for their
487 particular application and threat environment.

488 The CMVP validates specific versions of a cryptographic module, and the user must verify that
489 the version procured is in fact the validated version. The version numbers for a validated
490 cryptographic module are specified on the CMVP web site and in the latest Security Policy.

491 Users can also develop product or system specifications that include the requirements for FIPS
492 140-3 validated cryptographic modules. It is important to note that a cryptographic module may
493 be a complete product or a component thereof. Therefore, understanding the boundary and
494 interface of the validated cryptographic module will help in the determination of an adequate
495 cryptographic product.

496 2.7 CMVP Meetings

497 The CMVP is jointly managed by NIST and CCCS. Decisions are made jointly by both
498 organizations with the NIST and the CCCS Program Managers communicating regularly. While
499 most CMVP internal meetings focus on interactions with the CSTL, the CSTL Manager Meeting
500 is focused on assessments and improvements of the CMVP program operations and
501 management.

502 2.7.1 CSTL Manager Meetings

503 NIST and CCCS organize CSTL manager meetings (typically annually) to discuss issues relating
504 to the CMVP, CAVP, and CSTLs. An agenda is created and distributed to the CSTLs before the
505 meetings and presentation materials are distributed to the CSTLs for reference following the
506 meetings. CSTL managers are welcomed to add any new agenda items at any time. Typically,
507 the CSTL manager meetings are to include only CSTL managers and the CMVP and CAVP
508 Validation Authorities, however CSTL staff may be invited to attend, space permitting. It is
509 mandatory for CSTLs to have at least one attendee at the CSTL manager meeting.

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

- 511 • Status of the CMVP
- 512 • Changed or new CMVP processes and/or procedures
- 513 • Standards updates
- 514 • Laboratory accreditation process update news
- 515 • Implementation Guidance in development
- 516 • Status of the CAVP
- 517 • Test tool development
- 518 • Upcoming meetings and/or symposiums

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

522 2.7.2 CMUF participation

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

529 In recent years, CMUF has asked CMVP to attend and present at the scheduled (e.g., monthly)
530 meetings. In this way, CMVP has been able to communicate with both CSTLs and vendors to
531 define the planning and goals more clearly, while accepting feedback from the community. It has
532 also allowed CMVP to hear programmatic issues that vendors and CSTLs are experiencing or
533 anticipating in which CMVP may not have adequate awareness.

534 **2.8 Confidentiality of Information**

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

540 As required by the CSTL accreditation standards listed in Section 3.1 of this manual, CSTLs are
541 required to establish and implement procedures for protecting the integrity and confidentiality of
542 data entry or collection, data storage, data transmission and data processing. CSTLs must encrypt
543 and digitally sign cryptographic module validation test reports, and any proprietary information
544 when these documents are submitted to NIST and/or CCCS outside of Web Cryptik / Box.

545 NIST, CCCS, and the CSTLs must ensure that personnel joining or departing these organizations

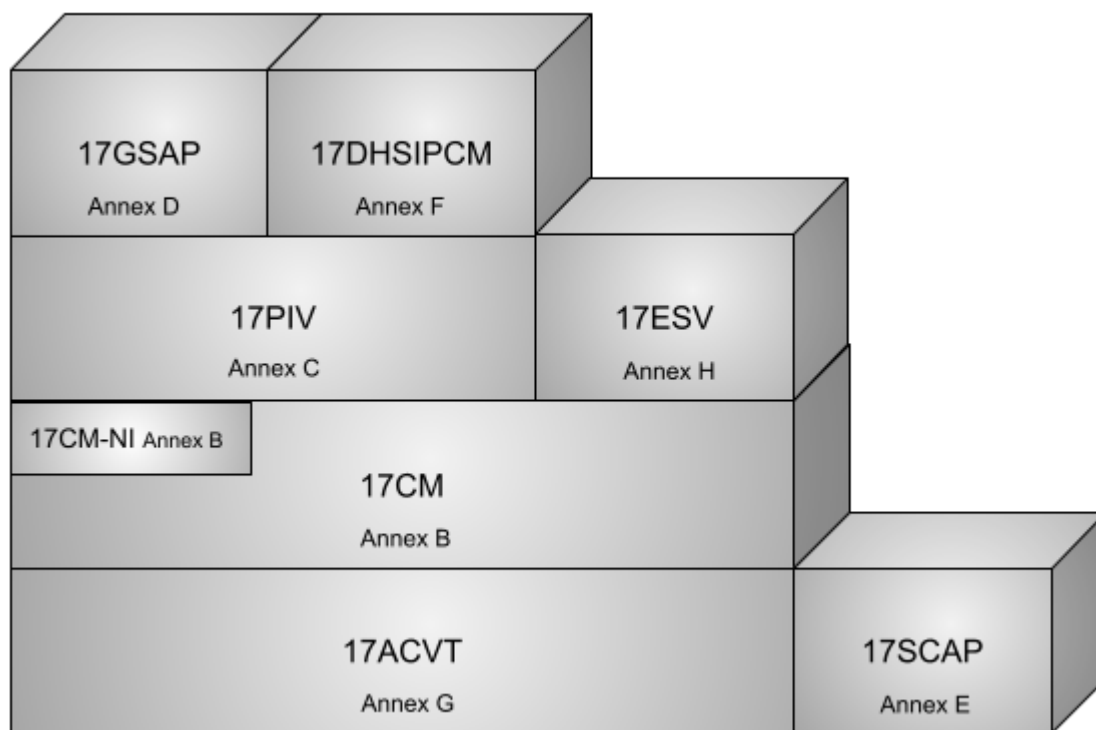
546 are advised of their responsibilities about safeguarding the vendor proprietary information they
547 may have been authorized to access during their period of employment.

548 **3 CSTL Processes**

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

552 **3.1 Accreditation of CMVP scopes for CSTLs**

553 This section describes in general terms the process for a laboratory to become an accredited
 554 CSTL for scope 17CM under the National Voluntary Laboratory Accreditation Program
 555 (NVLAP). Candidate laboratories may optionally apply for NVLAP 17CM-NI at the same time.
 556 17ESV is also supported by CMVP, though is considered a separate program. Laboratories are
 557 responsible for complying with the Cryptographic and Security Testing LAP which can be found
 558 at <https://www.nist.gov/nvlap/cryptographic-and-security-testing-lap>.



559
 560 *Figure 2 - CSTL NVLAP scopes*

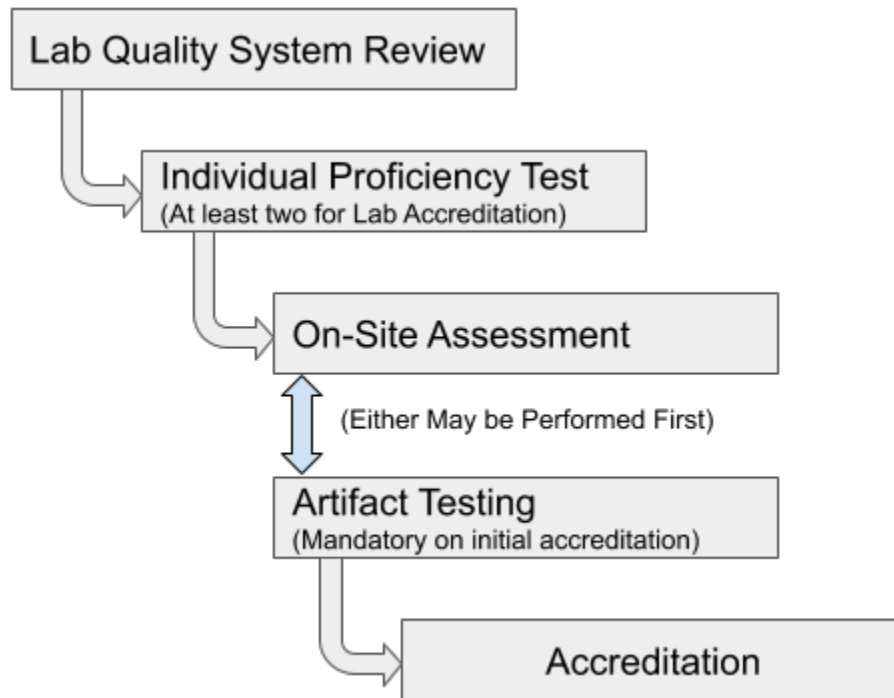
561 **NOTE:** Accreditation of the CAVP scope is necessary to obtain the 17CM scope for CMVP
 562 testing laboratories. For more information about CAVP accreditation, please see **Becoming a**
 563 **17ACVT Laboratory** on the CAVP website [https://csrc.nist.gov/Projects/cryptographic-](https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/how-to-access-acvts)
 564 [algorithm-validation-program/how-to-access-acvts](https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/how-to-access-acvts).

565 3.1.1 Accreditation Process for the CMVP scope

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

567 submission of the NVLAP application. Applications that are not completed within one year will
 568 have to be re-submitted and the process started again from the beginning. If the content of the
 569 accreditation process contained herein diverges from the aforementioned standards documents,
 570 those documents have precedence.

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



573
 574 *Figure 3 - CSTL Accreditation Process*

575 3.1.1.1 Application for Accreditation and Selection of Assessment Team

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

584 3.1.1.2 Management System Evaluation

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

587 3.1.1.3 CVP Proficiency Examination

588 Every independent tester, technical reviewer and submission signatory **shall** maintain
 589 Cryptographic Validation Program (CVP) certification by passing the current proficiency exam.

590 The current written examination consists of approximately one hundred questions relating to
591 various aspects of CSTL activities, FIPS 140-3, and cryptographic algorithm implementation
592 testing. The exam is an individual certification exam administered by a third-party organization.
593 The certification exam will encompass the domains listed below:

- 594 • Physical Security
 - 595 ○ Understand the different module types and different embodiments for
596 modules.
 - 597 ○ Understand requirements for physical security for modules specific to levels 1-
598 4.
- 599 • Authentication, Roles, Services, Software/Firmware Security and Operational
600 Environment
 - 601 ○ Understand authentication requirements and concepts.
602 ○ Define the requirements for roles.
- 603 ○ Understand the concepts of services using approved and non-approved604 functions, and the bypass capability.605 ○ Understand the self-initiated cryptographic output capability,606 Software/Firmware security including loading requirements and their607 applicability.608 ○ Describe the operational environment requirements/concepts and how to test609 them.
- 610 • Algorithms and Self-Tests
 - 611 ○ Understand the concepts of the approved and allowed algorithms.
612 ○ Identify which algorithms are approved or allowed.
- 613 ○ Identify testing for components of the algorithms.614 ○ Identify the tester's responsibilities when reviewing an algorithm's615 implementation.616 ○ Identify the pre-operational self-tests (e.g., integrity, bypass) and know the617 associated requirements.618 ○ Understand the requirements for conditional self-tests, including cryptographic619 algorithm self-tests.
- 620 • Sensitive Security Parameter (SSP) Establishment
 - 621 ○ Understand the requirements for SSP generation, SSP agreement, SSP
622 transport and SSP derivation and applicable standards and guidance.
- 623 ○ Understand and identify the approved random bit generators.624 ○ Understand the notion of entropy and methods of entropy estimation.625 ○ Possess general knowledge of the SSP establishment protocols and standards626 in the IT industry.

- 627 • SSP Management
 - 628 ○ Understand the requirements for SSP entry and output and trusted channels.
 - 629 ○ Understand the requirements for SSP storage.
 - 630 ○ Understand the various types of SSPs and their zeroization requirements.
- 631 • Security Assurances
 - 632 ○ Understand the requirements of module specification including degraded
 - 633 operation, approved and non-approved modes.
 - 634 ○ Understand the programmatic guidance and associated documentation
 - 635 requirements.
 - 636 ○ Understand the requirements for ports & interfaces, finite state model,
 - 637 development, mitigation of non-invasive and other attacks, and design
 - 638 assurance.

639 The exam is graded by an independent testing organization, and the results are provided to the
 640 CMVP. Scoring is adjusted for the difficulty of the exam taken, but transparent to the tester. The
 641 reexamination period for maintaining the certification for CVP certified testers is four years. In
 642 the event of major program updates, e.g., a new FIPS 140 standard, the reexamination frequency
 643 may be increased to encompass changes in the technical requirements. For the most up to date
 644 information, refer to the CVP Certification Exam Information tab on the CMVP website
 645 (<https://csrc.nist.gov/projects/cryptographic-module-validation-program>).

646 3.1.1.4 On-Site Assessment

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

652 If deficiencies are found during the assessment of an **accredited** CSTL, the laboratory must
 653 submit a satisfactory plan concerning resolution of deficiencies to NVLAP within thirty days of
 654 notification.

655 If deficiencies are found during the assessment of an **applicant** CSTL, the accreditation process
 656 may be allowed to continue, on the condition that the laboratory must submit a satisfactory plan
 657 concerning resolution of deficiencies within thirty days of notification.

658 3.1.1.5 Artifact Testing

659 After two testers pass the CVP exam or following the on-site assessment, the assessment team
 660 may provide an artifact that the applicant laboratory must test according to the policies of the
 661 CMVP. Once completed, the applicant laboratory must submit the test report to the CMVP for
 662 their review. The CMVP will then assess the competency of the laboratory using the responses
 663 provided in the test report. The initial NVLAP application includes the testing of the artifact, all
 664 of which must be completed within one (1) year.

665 3.1.1.6 Accreditation Decision

666 The CMVP will make a recommendation to grant or deny the accreditation of the applicant
667 laboratory. NVLAP will evaluate the results of the report on the laboratory and the
668 recommendations of the CMVP, including any deficiencies and the corresponding response by
669 the CSTL, before making the final accreditation decision.

670 3.1.1.7 Granting Accreditation

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

- 673 • January 1
- 674 • April 1
- 675 • July 1
- 676 • October 1

677 The accreditation period is one year. After initial accreditation, NVLAP will conduct an on-site
678 assessment during the first year of accreditation and then every two years (see NIST HB 150,
679 3.2.3.3). The CSTL receives a NVLAP certificate and scope of accreditation identifying the
680 CSTL address, lab code, the CSTL's authorized representative, and the expiration date of the
681 accreditation.

682 3.1.1.8 CMVP Test Tools

683 Once accreditation has been granted and the CMVP is advised by NVLAP that the applicant
684 laboratory has been accredited, the CMVP will issue to the newly accredited CSTL access to the
685 latest version of Web Cryptik and associated tools. CMVP will also issue the latest
686 programmatic directives and policies, and internal guidance and documentation. The CSTL is
687 also required to have secure email capability using PGP to encrypt any IP communications that is
688 not covered by Web Cryptik. The lab is limited to two PGP email addresses in which to
689 communicate with the CMVP, of which one may be a shared email address within the CSTL.
690 PGP is not provided by the CMVP.

691 3.1.1.9 Cooperative Research and Development Agreement

692 All accredited CSTLs must execute a Cooperative Research and Development Agreement
693 (CRADA) agreement with NIST in order to do business with the CMVP. The agreement covers
694 protection of information as well as the fees being charged by NIST for each type of CMVP test
695 report submission (scenario). This agreement is effective through October 31, 2026. The
696 agreement may be reviewed and revised on an as needed basis. New laboratories are required to
697 execute the agreement once they become accredited through NVLAP. Existing laboratories must
698 re-execute the agreement upon change or expiration. The NIST CMVP Program Manager is the
699 point of contact for obtaining a copy of the current CRADA.

700 **3.2 Maintenance of CSTL Accreditation**

701 3.2.1 Proficiency of CSTL

702 There is no requirement for a test report submission during the first year of accreditation. For all
703 successive years of accreditation, the following requirements apply. An accredited CST
704 laboratory must submit a minimum of three (3) test reports within the two-year period of the

705 accreditation date. The laboratory must submit a minimum of one (1) test report within each
706 successive one-year accreditation cycle. For more information, see HB 150-17 Section B.3.5.3
707 *Minimum number of vendor product test reports.*

708 This permits the CMVP staff to monitor the quality of the laboratory processes, and the technical
709 skills and knowledge of the laboratory staff. Failing this, NVLAP may suspend or revoke the
710 laboratory's accreditation.

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

713 3.2.2 Renewal of Accreditation

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

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

724 3.2.3 Ownership of a CSTL

725 In the event a CSTL changes ownership, the accreditation body and the CMVP Validation
726 Authorities must be informed within ten working days of the identity of the new owner of the
727 laboratory and the effective date of the change. The laboratory must also submit an updated
728 Quality System to NVLAP showing the new owner information.

729 3.2.4 Relocation of a CSTL

730 In the event a CSTL relocates to a new facility, the laboratory director must submit a relocation
731 plan to the accreditation body and the CMVP at least one month before the relocation. The
732 relocation plan must demonstrate that the new location meets the requirements as set out in the
733 accreditation standards including information protection. The plan must also describe how
734 sensitive information will be moved between locations. The accreditation body and the CMVP
735 staff may conduct a monitoring visit after the relocation is completed to ensure all accreditation
736 requirements continue to be met.

737 3.2.5 Change of Approved Signatories

738 In the event of a change of the CSTL's Approved Signatories, the accreditation body and the
739 CMVP must be informed within thirty working days of the new signatories and the effective date
740 of the change. All approved signatories must have passed the CVP exam prior to signing a
741 validation submission.

742 3.2.6 Change of Key Laboratory Testing Staff

743 Key personnel include:

- 744 • laboratory director;
- 745 • laboratory manager(s);
- 746 • staff members(s) responsible for maintaining management system;
- 747 • authorized representative;
- 748 • approved signatories; and
- 749 • other key technical persons in the laboratory (e.g., testers).

750 In the event of changes to key laboratory testing staff, the accreditation body and the CMVP
 751 must be informed of the new staff and the effective date of the change within thirty working
 752 days. Failure to communicate laboratory staff changes to the accreditation body and the CMVP
 753 may result in an adverse action regarding accreditation. The laboratory must submit an updated
 754 organizational chart to NVLAP and the CMVP noting any changes.

755 3.2.7 Monitoring Visits

756 Monitoring visits may be conducted by the accreditation body at any time during the
 757 accreditation period, for cause or on a random basis. While most monitoring visits will be
 758 scheduled in advance with the laboratory, the accreditation body may conduct unannounced
 759 monitoring visits. The scope of the monitoring visits may range from an informal check of
 760 specific designated items to a complete review.

761 3.2.8 Suspension, Denial and Revocation of Accreditation

762 If the accreditation body becomes aware that an accredited laboratory has violated the terms of
 763 its accreditation, it may suspend the laboratory's accreditation or advise the laboratory of their
 764 intent to revoke the accreditation. The determination by the accreditation body whether to
 765 suspend the laboratory or to propose revocation of a laboratory's accreditation will depend on the
 766 nature of the violation(s).

767 Potential violations include but are not limited to, not performing tests in accordance with the
 768 standards, inadequate maintenance of CSTL equipment, or persistent process or technical
 769 shortfalls. An accredited laboratory **shall** maintain an Extended Cost Recovery (ECR) point total
 770 of less than 12 points. If a laboratory accumulates 12 or more points during the previous 2-year
 771 period, the accreditation for the cryptographic module testing will be suspended.

772 If a CSTL has reached 6 or more points through the ECR process in the past two years, in order
 773 to pre-empt a NVLAP suspension of the CMVP scope should the lab accrue additional ECR
 774 points, the CMVP recommends the following actions:

775 The lab compile a list of all reports in the Review Pending state in the CMVP queue. Per
 776 policy, those reports are eligible for resubmission. If the CSTL elects to review those
 777 submissions for potential resubmission, the CMVP may initiate up to a 30-day HOLD to

778 allow the CSTL time to make any corrections needed prior to the reports moving to the In
 779 Review state. The CMVP would need to be notified in writing regarding which reports,
 780 if any, the CSTL would like to put on HOLD pending a resubmission. The final
 781 determination will be up to the CMVP.

782 ECR points are levied as follows:

783 0 points - Excessive number of modules in one report, or excessive submission size
 784 and/or complexity. Or for special exception requests received from the labs
 785 that create extra work for the CMVP.

786 1 to 4 points - Excessive comments; excessive comment rounds; missing, incomplete, or
 787 inconsistent documentation

788 5 points - Nonconformities such as a security-related issue or inaccurate representation of
 789 a module

790 Laboratories that fail to maintain a minimum of two CVP certified testers during their
 791 accreditation cycle will be suspended.

792 Discovery of serious violations such as breach of information confidentiality will result in an
 793 immediate recommendation by the CMVP to the accreditation body to suspend the CSTL's
 794 accreditation while an investigation is conducted, and necessary corrective actions are taken.

795 3.2.9 Voluntary Termination of the CSTL

796 A CSTL may at any time terminate its participation and responsibilities as an accredited
 797 laboratory by advising the accreditation body and the CMVP Validation Authorities in writing of
 798 its intent. Upon receipt of a request for termination, the accreditation body **shall** begin the
 799 termination process by notifying the laboratory that its accreditation has been terminated. The
 800 laboratory will be instructed to return its Certificate and Scope of Accreditation and to remove
 801 the accreditation body's logos from all test reports, correspondence, and advertising. Finally, the
 802 laboratory **shall** return or provide signed confirmation of the destruction of all CMVP and CAVP
 803 provided material, test tools and documentation. The CMVP will determine the course of action
 804 taken for any outstanding work that has not been completed. This will be handled on a case-by-
 805 case basis.

806 3.3 Confidentiality of Proprietary Information

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

809 3.3.1 Confidentiality of Proprietary Information Exchanged between NIST, CCCS and the CSTL

810 The confidentiality of the proprietary information exchanged between NIST, CCCS and the
 811 CSTL is required by the NVLAP at all times during and following the testing. All proprietary
 812 materials must be marked as PROPRIETARY by the CSTL or the vendor.

813 3.3.2 Non-Disclosure Agreement for Current and Former Employees

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

816 **3.4 Code of Ethics for CSTLs**

817 The laboratory **shall**:

- 818 1) Maintain ISO/IEC 17025 NVLAP accreditation for the Cryptographic Security Testing
819 Program;
820 2) Refrain from misrepresenting the scope of its accreditation;
821 3) Act legally and honestly;
822 4) Act ethically.

823 **3.5 Management of CMVP and CAVP Test Tools**

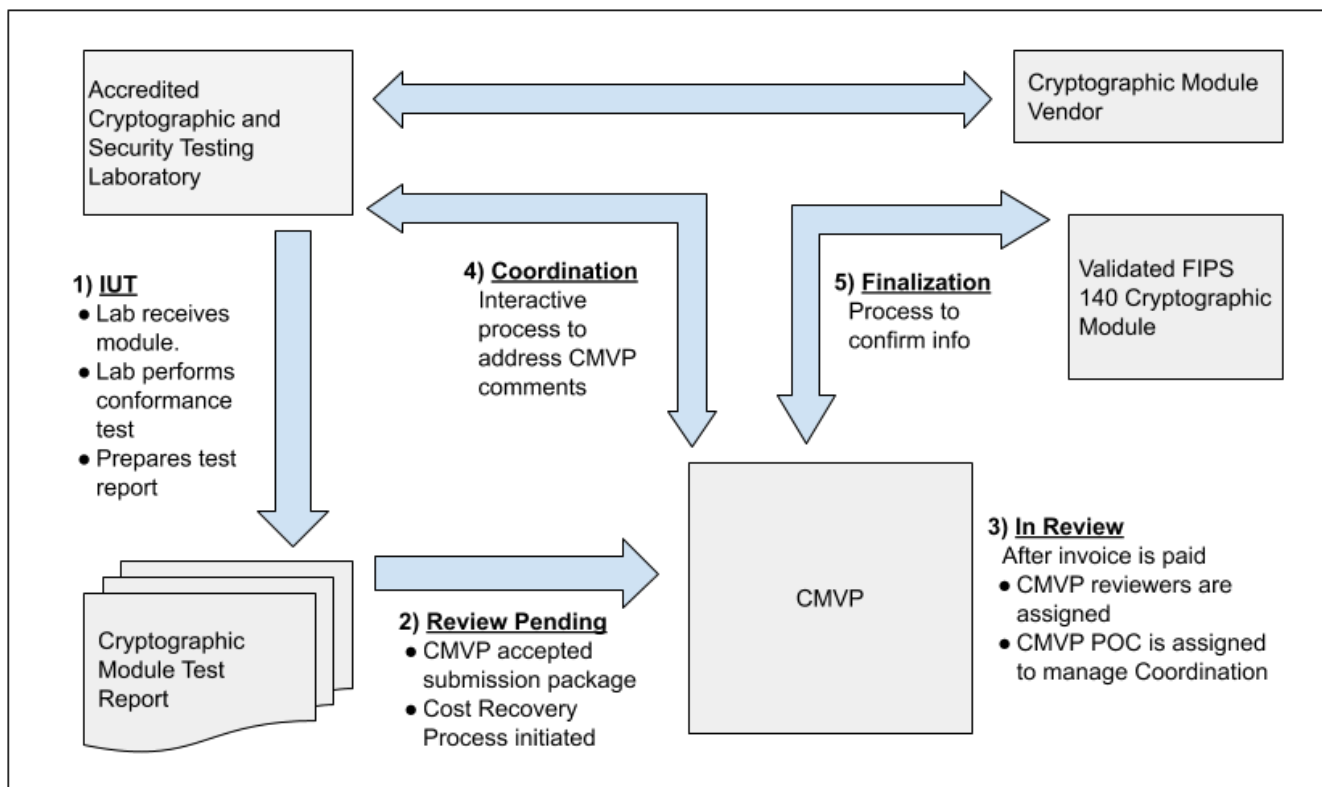
824 Test tools provided by NIST and CCCS **shall** not be distributed to any entity outside the CSTL,
825 including firms contracted by the CSTL, unless explicitly authorized by CMVP management.
826 Personnel temporarily employed by and working under the supervision of a CSTL (i.e., a
827 contractor) can use the provided test tools when they are used within the CSTL facilities. Test
828 tools include all versions of Web Cryptik, the Automated Cryptographic Validation Testing
829 System (ACVTS) and any other tools developed by NIST and CCCS for use by the CMVP and
830 CAVP. Violation of this policy may be considered cause for suspension of the CSTL's
831 accreditation.

832 **4 CMVP Processes**

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

835 **4.1 Cryptographic Module Validation Process Overview**

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



841
 842 *Figure 4- Cryptographic Module Testing and Validation Process*

843 **4.1.1 Vendor, CSTL, and CMVP duties for Testing of the Cryptographic Module**

844 A vendor contracts with an accredited CSTL to perform the cryptographic module validation
 845 testing. The vendor provides the laboratory with the necessary documentation and either
 846 provides the cryptographic module to the laboratory for testing or prepares it for testing at the
 847 vendor’s facility.

848 In order to communicate specific validation information to CMVP, the CSTL **shall** assign a
 849 Tracking Identification Number (TID). The first two digits of the TID are assigned by the CMVP
 850 once laboratory accredited, the second set of four digits is assigned by the laboratory which must

851 be unique to the validation, and the last four digits are “0000” unless otherwise specified, when
852 the validation submission is accepted. In all, a ten-digit TID number is created and used to track
853 the submission. Most communications with the CMVP are aided by the use of Web Cryptik with
854 attachments as indicated in the Web Cryptik User Guide. For the latest information refer to the
855 Web Cryptik User Guide.

856 4.1.1.1 Implementation Under Test

857 Once the documentation is delivered to the laboratory and the cryptographic module is available
858 for testing, and with the vendor’s agreement, the laboratory may optionally notify the CMVP that
859 the cryptographic module is to be included on the IUT List. The laboratory provides the name of
860 the cryptographic module and the cryptographic module vendor’s name and indicates that this
861 information is to appear in the IUT List. Inclusion in this list is voluntary. The module on the
862 IUT List will be removed after 18 months. The CSTL will be notified when the IUT is dropped.

863 The CSTL performs the cryptographic module testing as prescribed by the ISO/IEC 24759:2017
864 Test Requirements, SP 800-140 and applicable IGs, entering all testing assessments in the Web
865 Cryptik tool. Although testing requirements are in the ISO/IEC 24759:2017 TR, ISO/IEC
866 19790:2012, *Security Requirements for Cryptographic Modules* remains the definitive reference
867 for whether or not the cryptographic module meets the requirements of the standard. The SP 800-
868 140 series and Implementation Guidance (IG) provides clarifications of the CMVP, and in
869 particular, clarifications and guidance pertaining to the TR. Cryptographic algorithm and/or
870 entropy source validation testing may also need to be done as part of the FIPS 140-3 validation
871 testing.

872 The cryptographic module validation process is an iterative process. At any point in the testing
873 the CSTL may wish to request guidance from CCCS and NIST in determining how to apply the
874 FIPS 140 standard to the particular cryptographic module. If the CSTL discovers any non-
875 conformances in the cryptographic module documentation or the cryptographic module itself, it
876 must bring details of the non-conformance(s) to the attention of the cryptographic module
877 vendor. The cryptographic module vendor must correct the non-conformance(s) and resubmit
878 updated documentation and the updated cryptographic module as necessary for validation
879 testing.

880 Once the CSTL completes all required validation testing and has determined that the
881 cryptographic module is conformant to FIPS 140-3, the laboratory prepares the validation
882 submission and sends it to CMVP for validation. In responding to assessments through Web
883 Cryptik, the CSTL addresses each TE independently, not by referencing a response in another
884 TE. Having to search and piece together information increases the CMVP review time and may
885 facilitate a NIST ECR Fee and possible points.

886 See the Web Cryptik User Guide for a summary table that describes what must be submitted by
887 the laboratory for validation. Web Cryptik aids the CSTL in preparing submissions, please refer
888 to the Web Cryptik User Guide for additional information.

889 4.1.1.2 Review pending

890 All FIPS 140 validation submissions received by the CMVP are examined to assure a full
891 package was received. If the initial examination reveals issues, the CSTL is notified, and the
892 submission is not accepted for review. When the submission is accepted by the CMVP, the
893 module is moved to the REVIEW PENDING stage of the MIP List. The module will remain in

894 the REVIEW PENDING stage until the NIST Cost Recovery fee is paid and the first reviewer
895 begins the review.

896 At the CMVP's discretion, a test report in this state may be subject to a triaged review that is
897 used to quickly assess the quality of a report, and if needed, provide feedback to the lab. This
898 triage activity is implemented based on common issues observed from the submissions received
899 by the CMVP. Ability to quickly identify and address problematic submissions is paramount to
900 not only advance the FIPS 140-3 queue, but also be fair to all labs and vendors. Problematic
901 submissions will be sent back to the labs accompanied by generic statements for resolution.
902 These reports *will* maintain their respective queue positions.

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

906 4.1.1.3 In Review

907 After the CMVP reviewers have been assigned to the submission, and the reviewer begins the
908 review, the cryptographic module is moved to the IN REVIEW stage of the MIP List. The
909 module validation must be completed and cannot exceed 24 months after transitioning to IN
910 REVIEW. Once they have completed their review of the validation submission and provided
911 comments, a comment file is sent to the CSTL. This event moves the cryptographic module to
912 the COORDINATION stage, described in Section 4.1.1.4. During long submission queues, the
913 CSTL may ask for minor updates that would otherwise require a revalidation submission to be
914 incorporated into the current submission. CMVP will consider this and will respond in a timely
915 fashion.

916 4.1.1.4 Coordination

917 After receiving the comments from the CMVP and conferring with the vendor, as necessary, the
918 CSTL addresses the comments and resubmits a complete submission package containing any
919 modified documents. The reviewers examine the responses and respond with any additional
920 comments if necessary. Additional rounds due to errors or complex issues may result in a NIST
921 ECR Fee and possible points. This process continues until the CSTL receives an All OK from
922 the CMVP. Each round of comments will result in an update in the MIP List Coordination date.
923 The CSTL must respond within 90 days to prevent the review being placed on hold. Also, see
924 [Section 4.4.6 Changes while in Coordination](#) for more information.

925 4.1.1.5 Finalization

926 The FINALIZATION stage focuses on assuring any changes during the coordination phase have
927 been updated by the CSTL. In addition, the CSTL is asked to review and confirm with CMVP
928 the vendor and module information is accurate. With the completion of the submission review,
929 the validation is posted on the CMVP website.

930 4.1.1.6 Validation Certificate

931 When NIST and CCCS are satisfied with the test report, the finalized comment file and the
932 electronic version of the draft validation certificate is sent to the CSTL. The CSTL must review
933 and confirm or correct the information on the certificate. Once the information is confirmed, the
934 Validation Authorities, issue a certificate number which is added to the database. The web-based
935 search tool for the database can be found at <https://csrc.nist.gov/Projects/cryptographic-module->

936 [validation-program/validated-modules/Search](#). An entry includes the version number of the
937 validated cryptographic module and benchmark configuration of the original validation testing.

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

946 **4.2 Implementation Under Test (IUT) and Modules in Process (MIP)**

947 The *CMVP Implementation Under Test (IUT) and Modules In Process (MIP) Lists* are provided
948 for information purposes only. Participation on the list is *voluntary* and is a joint decision by the
949 vendor and the CSTL. Modules are listed alphabetically by name.

950 The IUT List provides the Module Name, Vendor Name, FIPS 140 standard and the date of the
951 last update from the CSTL under contract to perform the testing. Not all modules being tested are
952 listed, as the listing is optional.

953 Similarly, if a vendor and CSTL chose not to list the module on the MIP List, the module will be
954 reflected at the end of the list in the “Not Displayed” row. If the CSTL requests the listing be
955 posted, the Module Name, Vendor Name (and expandable contact information), FIPS 140
956 standard, and the submission status (including the current MIP state and the date of the last MIP
957 state change) will be shown. Posting on the list does not imply or guarantee FIPS 140 validation.

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

960 **4.3 Submission Scenarios**

961 There are twelve possible FIPS 140-3 submission scenarios:

962 Full Submission (FS), Vendor Update (VUP), Vendor Affirmed Operational Environment
963 (VAOE), Non-Security Relevant (NSRL), Algorithm Update (ALG), Operational Environment
964 Update (OEUP), Rebrand (RBND), Port Sub Chip (PTSC), Update (UPDT), Common
965 Vulnerabilities and Exposures (CVE), Algorithm Transition (TRNS), and Physical Enclosure
966 (PHYS). See [Section 7.1](#) for details for each of these scenarios.

967 **4.4 Validation Submission Queue Processing**

968 **4.4.1 Full and Update Submission Validations**

969 Modules submitted for initial validation (FS) and those submitted with less than 30% security
970 changes (UPDT) will be queued together and addressed on a first-come, first-serve basis. All
971 submissions in this queue must meet all requirements as of the submission date. The internal

972 review disposition of a module report is left to the sole discretion of the NIST and CCCS CMVP
 973 program managers. If additional time is required due to complexity or errors, additional cost and
 974 possible points may be required in the form of a NIST ECR. The status of these submissions can
 975 be tracked through the MIP List on the webpage at [https://csrc.nist.gov/Projects/cryptographic-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List)
 976 [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). Vendors should work
 977 with their CSTL for any additional information.

978 In cases whereby submissions are related to or dependent on other submissions, especially for
 979 bound or embedded modules, the CMVP must be notified for consideration prior to their
 980 submission and added to the special instructions field in Web Cryptik. This will allow CMVP to
 981 manage resources in support of these larger efforts. If a submission is put on hold due to
 982 dependency, it is the responsibility of the lab to notify the CMVP when the initial submission is
 983 completed in order for the CMVP to remove the hold on related or dependent submissions. In
 984 general, and for dependent or related modules, testing must be completed prior to submission
 985 (including FIPS 140-3 compliance testing and CAVP/ESV validations).

986 4.4.2 All other submissions

987 Separate queue(s) are maintained by the CMVP internally to maximize throughputs for all other
 988 submissions, as they are expected to require less intense review and faster turnaround. If
 989 additional resources are required, an ECR Fee and possible points could be levied or a new
 990 submission as a full validation may be required.

991 4.4.3 HOLD Status for Cryptographic Modules on the Modules In Process

992 HOLD status can be initiated by the CMVP only. There are several reasons that a submission
 993 review may be placed on HOLD status. Some of these reasons are as follows:

- 994 1. If a module test report is sent incomplete or is determined to be incomplete once the
 995 module has moved to the IN REVIEW or a later stage, a NIST ECR Fee and points will
 996 apply. When the ECR notification is sent to the CSTL, the module will be placed on
 997 HOLD. If the ECR has been paid and the CSTL resubmits the report, the HOLD is
 998 removed.
- 999 2. If a non-compliance issue is discovered during module IN REVIEW or later a NIST
 1000 ECR Fee and points will apply. When the ECR notification is sent to the CSTL, the
 1001 module will be placed on HOLD. If the ECR has been paid and the CSTL resubmits the
 1002 report, the HOLD is removed.
- 1003 3. If a module is dependent on the completion of another module (i.e., the case of
 1004 bound/embedding), the dependent module may be placed on HOLD until the base
 1005 validation has been completed. The CSTL must indicate the module dependency upon
 1006 submission via Special Instructions.
- 1007 4. During COORDINATION, CMVP comments are sent to the lab and if the lab has not
 1008 responded within 90 calendar days, the module will be placed on HOLD and removed
 1009 from the MIP List. After 150 calendar days, an email notification will be sent to
 1010 indicate that if no submission is received in the next 30 calendar days (180 calendar
 1011 days in total), the module will be dropped from the CMVP queue. The lab must inform

1012 the vendor of the CMVP’s intent to drop the module due to the 6-month period of delay.
 1013 If the lab cannot respond to the CMVP Coordination comments within the allotted
 1014 timeframe, the lab must send an email justification to the CMVP identifying the reason
 1015 for this delay at least two weeks prior to the drop date. The lab must include a timeline
 1016 specifying the expected submission date for the CMVP’s consideration. If no
 1017 justification is received, the module will be dropped. A new submission could be sent
 1018 once this module has been dropped but cost recovery would be applicable.

1019 5. A CSTL has been placed in a suspension status by NVLAP. All work in progress may
 1020 be placed in a HOLD until the suspension is lifted. No new work is allowed to be
 1021 submitted during a period of suspension.

1022 6. The report was sent back to the CSTL with Triage comments that must be addressed
 1023 before the validation can continue. Once addressed, the CSTL sends an updated report,
 1024 and the modules moves back to the state it was in prior. See [Section 4.1.1.2 Review](#)
 1025 [pending](#) for more information on the Triage process.

1026 In general, a module that is on HOLD will be reflected on the MIP List as “On Hold”. The MIP
 1027 status will be the same after coming out of HOLD and will retain its position in the queue.

1028

1029 4.4.4 Validation Deadline

1030 CMVP drops modules from the queue that have not completed the validation process within 2
 1031 years from being placed in IN REVIEW status. The CSTL will be notified 30 days prior to the
 1032 termination of the submission. Should the modules approach the 2-year deadline, CSTLs have
 1033 the option to contact the CMVP for reconsideration; CMVP will consider factors that contribute
 1034 to the delay (e.g., if delay was not due to CSTL or vendor unresponsiveness / inadequacy in
 1035 addressing CMVP comments in a timely and efficient manner). When the module is dropped, the
 1036 vendor and lab must restart the validation process including paying a new cost recovery fee at the
 1037 current rate. This applies to all submissions currently in the process as well as to new
 1038 submissions.

1039 4.4.5 Resubmission while in Review Pending

1040 An updated submission (which will replace the original) may be provided to the CMVP while in
 1041 review pending if all the following rules are met:

1042 1. This is not to be used as a placeholder, and the initial submission must have been the
 1043 intended/desired version to be validated, with unforeseen and necessary updates.

1044 Penalties (e.g., ECR, or drop the module queue position) may be applied if misused.

1045 Acceptable (non-exhaustive) examples include:

1046 a. Updates to address CMVP checklist items or lessons learned from other module
 1047 validations. Documentation improvements are encouraged to ensure accurate,
 1048 high-quality reports and avoid ECR.

1049 b. Code changes that are necessary (e.g., address bug/CVE fixes) or strengthens the
 1050 module’s conformance claim (e.g., improve the granularity of the module’s show

1051 version service, or reduce potential ambiguity with the module's approved
1052 service indicators).

1053 c. Adding new OEs that were never originally intended/desired to be part of the
1054 validation.

1055 2. The updates must be allowed by and within the scope of the submission scenario, and
1056 full testing or regression testing may apply depending on the changes (see [Section 7.1](#)
1057 [Submission Scenarios](#)).

1058 The updated submission will keep its place in the queue.

1059 4.4.6 Changes during Coordination

1060 Changes during coordination are permitted if all the following rules are met:

1061 1. This is not to be used as a placeholder, and the initial submission must have been the
1062 intended version to be validated, with unforeseen and necessary updates. Penalties (e.g.,
1063 ECR, or drop the module queue position) may be applied if misused.

1064 2. Changes are purely documentary (no module code changes) UNLESS code changes
1065 are limited to one of the following:

1066 a. In response to CMVP comments.

1067 b. To address a CVE or other vulnerability.

1068 c. Non-security relevant bug fixes.

1069 d. To address an algorithm transition (i.e., one that would fit under scenario TRNS).

1070 3. The updates must be allowed by and within the scope of the submission scenario, and
1071 full testing or regression testing may apply depending on the changes (see [Section 7.1](#)
1072 [Submission Scenarios](#)).

1073 4. A detailed change summary is provided to the CMVP (may be part of the Comment
1074 document).

1075 Notes:

1076 a. Updates to improve documentation is encouraged to ensure accurate, high-quality reports
1077 and avoid ECR.

1078 b. The review may be delayed and an ECR may apply for complexity (time incurred)
1079 depending on the impact of the changes.

1080 c. Post-validation, additional changes can always be made using the revalidation scenarios
1081 per Section 7.1 of this document.

1082 4.5 Validation when Test Reports are not Reviewed by both Validation Authorities

1083 In rare occasions, laws from either country or other unusual circumstances prevent the release of
1084 product information outside its borders for specific products. In those occasions both Validation
1085 Authorities will be advised of the circumstances and the Validation Authority from that country
1086 will carry out the validation process on its own and will present the certificate to the other

1087 Validation Authority for its signature (where applicable).

1088 4.5.1 Controlled Unclassified Information

1089 If a CMVP test report is received from a CSTL and it is identified in the signed letter of
1090 affirmation that it is subject to the International Traffic in Arms Regulations² (ITAR), the
1091 following CMVP programmatic guidance will be adhered to:

1092 4.5.1.1 CMVP ITAR Guidance

- 1093 1. Report submission as specified in Web Cryptik applies and should include the following
1094 changes from a normal submission:
 - 1095 a. A proprietary security policy [PDF] submitted in lieu of a non-proprietary
1096 security policy.
 - 1097 b. Provide a signed letter of affirmation from the vendor stating the applicability
1098 of ITAR to the submitted test report.
 - 1099 c. To satisfy binding of Cryptographic Algorithm Validation Certificates, (see [IG](#)
1100 [2.3.A](#)), the test report must affirm that the CSTL has PDF images (front and
1101 back) for any ITAR cryptographic algorithm validation certificates, where the
1102 algorithm web site will not have any detailed information.
 - 1103 d. The test report package is submitted only to NIST CMVP. The TID field will
1104 be formatted as: TID-*nn-nnnn*-ITAR. The characters ITAR will replace the
1105 field that was allocated for the CCCS TID.
 - 1106 e. Actual module names, version numbers, and vendor information will be
1107 provided. This information will not be masked by dummy information.
- 1108 2. Report review
 - 1109 a. Each ITAR report will be reviewed by NIST reviewers.
- 1110 3. Certificate generation and posting
 - 1111 a. Certificates will be prepared by NIST only.
 - 1112 b. Certificates will be signed only by NIST. The CCCS signature field will be
1113 marked as: Not Applicable – ITAR.
 - 1114 c. The NIST CMVP web page will only post the following information:
1115 Certificate number, applicable FIPS standard, Status, Module Type,
1116 Embodiment, Validation Date, Sunset Date and Overall Level. It will also
1117 include the testing Lab and associated NVLAP Code.

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 criminal fines and penalties under Title 22 U.S.C. Section 2778, and Title 50, U.S.C. 2410. Recipient **shall** include this notice with any reproduced portion of this document.

1118 d. The official certificate will be sent to the CSTL for presentation to the vendor.

1119 4. Re-validation

1120 a. All re-validation changes will result in a new certificate sent to the CSTL for
1121 presentation to the vendor since the web site will not have any identifiable
1122 information.

1123 b. Report submission, report review, certificate generation and posting as outlined
1124 above and following the submission requirements.

1125 **4.6 CMVP Fees³**

1126 Fees are charged to the CSTL by NIST CMVP to offset the cost of the validation authority
1127 activities performed by NIST CMVP. Cost recovery fees are collected depending on the
1128 submission scenario as listed in [section 4.3](#). Extended Cost recovery fees are collected when the
1129 submission review is in excess of the allotted resources.

1130 4.6.1 Cost Recovery Fee

1131 Cost recovery (CR) is a fee charged to the CSTL by NIST CMVP to offset the cost of the
1132 validation authority activities performed by NIST CMVP. The fee is applied to new module
1133 submissions and modified module submissions.

1134 Fees charged by NIST as part of the cost recovery program are listed on:

1135 <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees>.

1136 4.6.2 Extended Cost Recovery Fee

1137 An extended cost recovery (ECR) fee is applicable when a report submission requires significant
1138 additional review effort by the validators. The extended fee may be applied to all report
1139 submissions. The CMVP will review the rationale for the application of the ECR fee and
1140 possible points with the CSTL before determination of its applicability. The ECR fee is billed
1141 separately from any applicable CR fee and must be remitted prior to validation. The ECR fee
1142 varies by submission type and security level.

1143 A number of factors may lead to an ECR fee and possible points:

1144 Complexity

1145 Typically, a report submitted by the CSTL to the CMVP addresses a single module. If the
1146 module represents a new technology, new type of fabrication or unique implementation, an
1147 unusual level of complexity and/or many functions and services; the review time will
1148 exceed the average and ECR will be applied.

1149 If the single report submission represents many modules, the review time will increase
1150 based on the quantity and module differences. If the review exceeds the average time an
1151 ECR will be applied or the report may be rejected unless the report is simplified, typically

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

1152 by reducing the number of modules to a more unified set.

1153 Additionally, technical issues resulting in a significant effort by CMVP to determine how
1154 new or unusual applications apply to the testing standards would result in the application
1155 of ECR.

1156 Quality

1157 Errors in the CSTL’s submission package or following an incorrect process can cause a
1158 significant effort by CMVP to identify and work with the CSTL to discover and correct.
1159 ECR will be applied.

1160 An ECR may be applied if, during CMVP review and coordination, the CSTL generates
1161 many responses that result in unproductive rounds due to issues in the report such as:
1162 incomplete information, inconsistent information, insufficient information, or not following
1163 CMVP Implementation Guidance or adherence to the conformance requirements. If
1164 significant or specialized effort is required by CMVP to resolve, an ECR will be applied. In
1165 addition, if during CMVP review and coordination it is discovered that the module is not
1166 conformant to FIPS 140 or CMVP Implementation Guidance, an ECR will be applied.

1167 Fees charged by NIST as part of the cost recovery program are listed on:

1168 <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees>.

1169 4.6.3 NIST Payment Policy

1170 NIST CMVP maintains the billing information for each CSTL. If the CSTL’s information needs
1171 to be updated, contact NIST CMVP. Upon receipt of the CSTL’s submission or a request for an
1172 invoice, NIST billing prepares an invoice and submits it to the identified payee. Only CSTLs
1173 with an active CRADA agreement will be invoiced by NIST billing. For questions about
1174 methods of payments and associated handling fees contact NIST Billing Information: 301-975-
1175 3880 or at billing@nist.gov.

1176 The NIST CMVP fee schedule is published at [https://csrc.nist.gov/Projects/cryptographic-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)
1177 [module-validation-program/nist-cost-recovery-fees](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees). Review of submissions will not begin until
1178 NIST CMVP receives confirmation from NIST Receivables that the invoice has been paid.

1179 4.6.4 Invoice for a Report Submission

1180 Currently, the CR process is initiated upon receipt of the report submission and typically adds an
1181 average of 60 days to the validation process. The CR process can be initiated before the report
1182 submission. In order to initiate the CR process, the lab **shall** send an IUTA (IUT-Add) using
1183 Web Cryptik indicating the correct number of modules, overall security level and submission
1184 type. The IUTA can be submitted without requesting that the module be placed on the IUT List.
1185 The IUTA must be successfully processed by the NIST CMVP automated system. When the
1186 submission is successfully processed, the lab will receive an automated response, “*Thank you for*
1187 *your submission*”.

1188 At any time after the lab receives the automated response to the IUTA, the lab has the option to
1189 send an IUTB (IUT-Billing) to initiate the CR process before submitting the report. When the
1190 IUTB is successfully processed, the lab will receive an automated response, “*Thank you for your*

1191 *request. The cost recovery process for this submission has been initiated.*” Changes to the overall
1192 security level and submission type will not be accepted.

- 1193 o If the lab sends an IUTB and then needs to cancel the invoice, the lab must send an
1194 IUTC (IUT-Cancel billing). When the IUTC is successfully processed, the lab will
1195 receive the automated response, “*Your request has been received and will be processed.*
1196 *If there are any issues in cancelling the invoice, you will be notified.*”
- 1197 o Once the invoice has been paid, the payment may be refunded if the module submission
1198 is dropped prior to the IN REVIEW stage.
- 1199 o Only the vendor.json file is required for an IUTB or IUTC. See the Web Cryptik help
1200 and User Guide for more information on this process.

1201 Labs should note when the cost recovery process starts, no changes to the Security Level or
1202 Submission Type will be accepted. In addition, if a report has not been received by 90 days after
1203 the IUTB was accepted, the module will be moved to On Hold and removed from the IUT List.
1204 The module can be automatically removed from On Hold and placed on the MIP List by sending
1205 the report. If the lab chooses to not send an IUTB, the CR process will initiate upon receiving the
1206 report submission.

1207 4.6.5 Request for Transition Period Extension

1208 Some Implementation Guidance is assigned a transition period before compliance to this
1209 guidance is required; since meeting the guidance may likely require changes to cryptographic
1210 modules or the functional testing of them as opposed to documentation changes. In some
1211 instances, the transition period may not be long enough for the vendor to perform the
1212 modifications needed to the cryptographic module for it to be compliant with the issued
1213 Implementation Guidance nor complete the additional cryptographic algorithm validation testing
1214 before the scheduled date for submission of the validation report.

1215 These situations will be reviewed on a case-by-case basis at the request of the CSTL performing
1216 the validation testing. A ruling will be made by the CMVP as to whether an extension can be
1217 granted for this particular requirement, for this particular cryptographic module, depending on
1218 the type of cryptographic module and the status of the validation testing.

1219 4.7 Flaw Discovery Handling Process

1220 When a flaw is discovered in a **validated** cryptographic module and brought to the attention of
1221 the CMVP Validation Authorities, the following actions will be taken:

- 1222 1. NIST, CCCS and the CSTL will investigate the allegation about the flaw, and
1223 determine its impact on the validation;
- 1224 2. NIST and CCCS will decide whether the flaw requires the revocation of the
1225 validation, a caveat be placed on the entry in the *Cryptographic Module Validation*
1226 *List*, or no action;
- 1227 3. NIST and CCCS may advise their respective federal departments of the flaw and its
1228 impact; and
- 1229 4. NIST and CCCS may notify NVLAP about the possible shortfall with the

1230 CSTL's proficiency.

1231 The diagram found in Annex A outlines the flaw discovery handling process. There are several
1232 ways for a flaw to be identified including a security-relevant CVE from the National
1233 Vulnerability Database (NVD).

1234 **4.8 Validation Revocation**

1235 FIPS 140 validation may be revoked for any one of the following reasons:

- 1236 1. Discovery of a flaw in a validated cryptographic module or that the cryptographic
1237 module was validated using false information; or
- 1238 2. Validated cryptographic module only implements cryptographic algorithm(s) that are
1239 no longer Approved.

1240 The entry in the *Cryptographic Module Validation List* will be annotated as follows for each of
1241 these cases:

- 1242 1. Discovered flaw; or
- 1243 2. Algorithm(s) no longer Approved for US Federal Government use: *No longer meets*
1244 *FIPS 140 requirements and can no longer be used by a Federal agency.*

1245 The Validation Authorities will jointly make the final decision on the validation revocation. The
1246 CSTL that performed the testing for the validation will be advised one week in advance of the
1247 upcoming validation revocation. If the validation certificate is revoked, it will appear on the
1248 *CMVP Validation List* with the validation status *Revoked*.

1249 **4.9 Entropy Source Validation (ESV) Processes**

1250 In April 2022, the CMVP introduced a new submission process for entropy sources leading to
1251 standalone entropy source validation certificates. The validation certificates provide the
1252 assurance that a particular entropy source on a particular operating environment conforms to SP
1253 800-90B and associated IGs.

1254 Similar to ACVTS, the CMVP maintains two environments: a Demo ESVTS, and a Prod
1255 ESVTS. The Demo environment is for testing and becoming familiar with the platform. The
1256 Prod environment is for certification.

1257 After December 2022, Prod ESVTS will be the only mechanism the CMVP allows on a new
1258 submission that requires a validation on an entropy source. Entropy source validation will no
1259 longer be accepted as part of a module submission (i.e., designated as ENT on the module
1260 certificate). Instead, the module submission must cite an existing entropy validation certificate.
1261 See Section 7.1.14 for additional information on ESV and ENT claims.

1262 4.9.1 Entropy Source Validation Submissions

1263 To submit to ESVTS, a client must be used to interact with the server. The CMVP provides two
1264 clients for use: an HTML-based WebClient, and a Python client. Both have their advantages and

1265 features. It is encouraged that a lab is familiar with both options.

1266 Several files are expected to be included in the submissions. It is the best practice to have these
1267 ready before making the initial request to ESVTS. The minimum set of files are as follows:

- 1268 1. Entropy Assessment Report (EAR) – This file addresses the requirements in SP 800-
1269 90B and describes how the entropy source on the listed operating environments conforms
1270 to the standard and associated IGs.
- 1271 2. Public Use Document (PUD) – This file provides information to a user that may
1272 incorporate or use the entropy source within a cryptographic module.
- 1273 3. Data Files – These are files described in SP 800-90B that capture outputs from the
1274 entropy source. The files are subject to the SP 800-90B Entropy Assessment Tool available
1275 on GitHub. The number of files required depends on the entropy source being evaluated.

1276 Part of the certify step (which is the last step of the submission to the ESVTS) is the inclusion of
1277 an Entropy Identifier (EID) that will help the lab track the submission as it goes through the
1278 review process. The EID must be four alphanumeric characters and must not repeat with
1279 previous EIDs used by the lab. This is similar to the TID used within the module review process.
1280 A string used as an EID may still be used as a TID and vice versa.

1281 After a submission is sent for certification the CMVP will perform cost recovery before the
1282 submission is passed along for manual review. During the manual review, two CMVP entropy
1283 reviewers will confirm the documentation provided addresses all of the SP 800-90B
1284 requirements.

1285 If the ESV submission is designated as ITAR:

- 1286 • Provide a signed letter of affirmation from the vendor stating the applicability of ITAR
1287 to the submitted report.
- 1288 • Use a client to submit the entropy assessment to the API and upload the corresponding
1289 data files. The description field can be modified.
- 1290 • Use nfiles to send the EAR, PUD, DCA, JSON metadata for ACVTS, and entropy
1291 assessment ID(s) to Chris Celi, christopher.celi@nist.gov.
- 1292 • Comment responses go ONLY to cmvpitar@nist.gov using PGP encryption. There is no
1293 ITAR flag in the EID.
1294

1295 An ESV certificate has a reuse status of either “Reuse restricted to vendor” or “Open for reuse”.

1296 “Reuse restricted to vendor” means:

- 1297 • Any module that has the same vendor can use the ESV certificate within their module
1298 with no additional permission, if the entropy source is portable to that module per the
1299 PUD guidance (e.g., identical environments, configuration steps, etc.).
- 1300 • The vendor’s name of the ESV certificate must match exactly with the module vendor
1301 name, unless the two vendors are part of the same company (e.g., different divisions with
1302 slightly different names, or a company is a subsidiary of another company that has a
1303 validation). This vendor relationship would need to be explained with evidence provided
1304 to the CMVP as part of the module submission.

1305 • Someone other than the vendor can only use the certificate with written and signed
1306 permission from the vendor’s point of contact (as indicated on the ESV certificate). The
1307 signed permission may be appended to the PUD of the certificate or be a separate
1308 document attached to the module submission package.

1309 “Open for reuse” means any vendor can use that certificate within their module without any
1310 specific permission from the ESV certificate vendor. It does NOT mean the vendor can rebrand
1311 the ESV as their own.

1312 4.9.1.1 Entropy Source Validation WebClient

1313 The WebClient provides forms that guide a submitter through the process. All information must
1314 be submitted at once including the EAR, PUD, and raw data files. Once a request is submitted to
1315 NIST, the user is expected to store the resulting output presented by the WebClient at the end of
1316 the submission. This provides a way to follow up on the request if needed. The URL to access
1317 the WebClient is the base URL of the ESVTS environment. The WebClient is available for both
1318 Demo and Prod. The Python Client can be downloaded from the URL indicated in the Entropy
1319 Source Validation Webpages (Section 4.9.3).

1320 4.9.1.2 Entropy Source Validation Python Client

1321 The Python Client provides a more automated way of submitting data to ESVTS. Requests may
1322 be made piecemeal when information becomes available. The user is expected to store the
1323 outputs from the tool. The tool automatically logs important information. The Python Client is
1324 controlled with JSON files to drive the functionality needed at the time. This allows a user to
1325 start making requests and pick them back up later. Configuration JSON files control if the
1326 Python Client is accessing Demo or Prod.

1327 4.9.2 Entropy Source Validation Comment Remediation Process

1328 When an entropy source submission is picked up for manual review, the lab will receive an email
1329 about the change in status of the submission. The reviewers will evaluate the claims made in the
1330 EAR, and evaluate the information provided in the PUD. If there are questions or comments
1331 about the submission, a file will be sent to the lab with PGP-encrypted email for further
1332 clarification. The email will have the subject line “EID-XX-YYYY-`{transaction code}`-yyMMddHHmm”
1333 where XX is the lab code, and YYYY is the four character EID provided during the certification
1334 request. On emails from the CMVP to the lab, the transaction code will be “CCOM#” where # is
1335 the number of comment rounds. For responses back to the CMVP, the lab must include the same
1336 subject line but the transaction code must be “LCOM#” where the # matches the latest number
1337 sent from the CMVP. Only the changed files are required in the response email.

1338

1339 4.9.3 Entropy Source Validation Webpages

1340 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)
1341 [module-validation-program/entropy-validations](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations).

1342 The ESV Certificate List is available on CSRC. See [https://csrc.nist.gov/Projects/cryptographic-
module-validation-program/entropy-validations/search](https://csrc.nist.gov/Projects/cryptographic-
1343 module-validation-program/entropy-validations/search).

1344 For access to the Python Client and ESVTS on Demo or Prod, see
1345 <https://github.com/usnistgov/ESV-Server>.

1346 4.10 CMVP Webpages

1347 This section provides information about the CMVP program that can be found on the web.

1348 4.10.1 Official CMVP Website

1349 The official CMVP website with all current publicly-available information on the CMVP is
1350 <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program>. It can also be reached
1351 through <https://nist.gov/cmvp>.

1352 4.10.2 Cryptographic Module Validation Lists

1353 The official CMVP website can generate the following lists related to the validation of
1354 cryptographic modules:

- 1355 • *Modules In Process* – A listing of the modules currently being reviewed by CMVP
1356 and the review state of each module. For more information about the MIP List, see
1357 section 4.2

1358 This list is updated as additional information is available. The validation process is a
1359 joint effort between the CMVP, the laboratory and the vendor and therefore, for any
1360 given module, the action to respond could reside with the CMVP, the lab or the
1361 vendor. This list does not provide granularity into which entity has the action.

- 1362 • *Implementation Under Test* – A listing of the modules currently being tested at the
1363 CSTL. This list is provided by the CSTLs and includes module name, vendor, FIPS
1364 140-2 or FIPS 140-3, and the date when added to the list.

1365 This list is updated as information is available. The IUT is under the control of the
1366 laboratory and the vendor. The CMVP is not aware of the submission schedule for
1367 these modules under testing.

- 1368 • *Cryptographic Module Validation Search can be found at:*
1369 [https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-
modules/Search](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-
1370 modules/Search)

1371 - A basic search supports a single overall list or a list resulting from a
1372 combination of vendor, module name, or certificate number. The basic search
1373 only addresses active modules.

1374 - An advanced search will generate a single list with the following options:

- 1375 • Certificate Number:
- 1376 • Vendor:
- 1377 • Module Name:

- 1378 • Standard: (FIPS 140-1, FIPS 140-2, or FIPS 140-3)
- 1379 • Module Type:
- 1380 • Validation Status: (Active, Historical, or Revoked)
- 1381 See the following web page for additional information
- 1382 [https://csrc.nist.gov/Projects/cryptographic-module-validation-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules)
- 1383 [program/validated-modules](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules)
- 1384 • Embodiment:
- 1385 • Year Validated:
- 1386 • Overall Security Level:
- 1387 • Algorithm:
- 1388 • Allowed Algorithms:
- 1389 • Tested Configuration:
- 1390 • Caveat:
- 1391 • Hardware Versions:
- 1392 • Software Versions:
- 1393 • Firmware Versions:
- 1394 • Lab:

1395 The search is updated when new validation certificates are posted to the website
 1396 for a cryptographic module or group of cryptographic modules, when validations
 1397 are extended to new versions of the cryptographic module through a revalidation,
 1398 or when a change is requested in the Vendor information, such as the Point of
 1399 Contact or the Vendor's Name. Only the current validation information is shown,
 1400 however, changes are indicated in the validation history.

1401 The lists are being improved as needs and time allows, so that more information
 1402 than indicated here may be available from these sources before the next update of
 1403 this document.

1404 4.10.3 CMVP Certificate Page Links

1405 Once the validation is identified, the information displayed typically includes vendor
 1406 information, module information, and required caveats. For each certificate there are also several
 1407 links from these pages that may be useful. These are described below.

1408 4.10.3.1 Security Policy

1409 This link is connected to the security policy that is the vendor provided summary of the
 1410 capabilities and security information of the module in a PDF format. The file is created under the
 1411 agreement from the vendor and is available from the CMVP website.

1412 4.10.3.2 Consolidated Validation Certificate

1413 This link is connected to a list of certificates that were issued for the month of interest. It
 1414 provides summary information that is accurate at the time of signing. For the latest module
 1415 information, please refer to the certificate page. The file is created by CMVP and is from the
 1416 CMVP website. Recent validations may not have this link available until the consolidated

1417 certificate process can be completed.

1418 4.10.3.3 Vendor Link

1419 This link is provided by the vendor to CMVP. The vendor is responsible for the accuracy of the
1420 link and the content. The CMVP does not endorse the views expressed or the information
1421 presented in the directed link, nor does it endorse any commercial products that may be
1422 advertised or available at the directed link.

1423 4.10.3.4 Vendor Product Link

1424 The purpose of this web link is for vendors to provide a concise listing of known products which
1425 incorporate their validated cryptographic module or, if the cryptographic module is a standalone
1426 product, additional relevant information about the product. The CMVP hopes that this link will
1427 make it easier for potential customers and users to identify products that use validated
1428 cryptographic modules.

1429 The link in the certificate details page is to a vendor provided URL that is vendor created and
1430 vendor maintained. The provision of this Vendor Product Link by the vendor is optional. The
1431 CMVP does not endorse the views expressed or the information presented in the directed link
1432 nor does it endorse any commercial products that may be advertised or available at the directed
1433 link. Press releases are not accepted.

1434 4.10.3.5 Algorithm Certificates

1435 Links to the CAVP validation certificate for the approved algorithms used in the module are
1436 provided for those wishing to know more details to the specific testing performed. The link is
1437 from the CAVP website. This currently is under development and may change. Algorithm
1438 validation certificates can also be found in the security policy.

1439 4.10.3.6 Validation History

1440 The initial validation and all updates are shown along with the CSTL responsible. The validation
1441 shown includes all updates and is considered the official validation. If information concerning a
1442 revalidation is needed, contact the CSTL indicated on the validation certificate.

1443 4.10.3.7 Usage of FIPS 140-3 Logos

1444 Once validation is achieved CMVP will forward through the CSTL to the Vendor instructions
1445 about the use of the NIST FIPS 140-3 logo. Vendors who use validated modules in their products
1446 may also request use of the NIST FIPS 140-3 Logo. The request instructions and use
1447 requirements is available from the CMVP web site: [https://csrc.nist.gov/Projects/cryptographic-
1448 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
1449 cmvp@nist.gov.

1450 **5 CMVP and CAVP Programmatic Metrics Collection**

1451 This section provides an overview of the CMVP and CAVP Programmatic Metrics Collection
1452 and a description of the collection and reporting processes of the CMVP metrics.

1453 **5.1 Overview**

1454 The CMVP Programmatic Metrics Collection process is intended to document the quality
1455 performance of the testing and validation processes of the CMVP and to allow the program to
1456 evaluate its relevance within the government. To achieve these objectives various metrics are
1457 collected through the testing and validation processes of the CSTLs and the CMVP. These
1458 metrics are intended to identify general programmatic trends and not to measure individual
1459 laboratory or vendor performances.

1460 **5.2 Confidentiality of the Collected Metrics Data**

1461 The CMVP considers the data collected and reported by the individual CSTLs as proprietary.
1462 CMVP makes every effort to anonymize the information by sampling only larger data sets and
1463 combining them without tracking information. The statistical information derived from the
1464 collected data is considered to be non-proprietary.

1465 **5.3 Collected Metrics**

1466 With the migration to FIPS 140-3 and the changes in the collection tools, we are currently
1467 reevaluating the methods used to collect useful metrics. Though the program will likely follow
1468 much of the previous procedures, it is not possible at this time.

1469 6 Test Tools

1470 This section covers the testing tools CSTLs are expected to utilize in the testing and reporting of
 1471 validation submissions. Where applicable, the title of the person responsible for the update
 1472 and/or maintenance of the document is identified.

1473 6.1 Web Cryptik

1474 Web Cryptik is a required tool for the completion of module testing, and generation of
 1475 documents that **shall** be included in a formal submission from the CST. The Web Cryptik tool is
 1476 to be used to record details of the cryptographic module being tested, the specific testing
 1477 performed, and the results of the validation testing. It is also to be used to create, among other
 1478 documents, the FIPS 140 validation test report and draft certificate. Information about new
 1479 features, enhancements, and bug fixes are provided with each release of the tool in the Web
 1480 Cryptik User Guide.

1481 Most submissions to CMVP are done through the use of Web Cryptik. The Web Cryptik User
 1482 Guide provides a summary table of the submissions supported by Web Cryptik and files that
 1483 must be included with the submission.

1484 For some submissions that are not handled by Web Cryptik, such as RFGs, but do contain IP,
 1485 PGP should be utilized.

1486 **Responsible Individual:** NIST CMVP Program Manager.

1487 6.2 Suggested Tools for Physical Testing

1488 As indicated in HB 150-17 Section B.6.4.2, a CSTL **shall** meet the minimum hardware and
 1489 software requirements for physical security testing. The CSTL can determine which tools to use
 1490 to meet the requirements, however, below is a suggested tool list:

1491 X-Acto or Utility "Type" knives (including various blades)
 1492 Strong artificial light source (Wavelength range of 400nm to 750nm)
 1493 Magnifying glass
 1494 Dremel "Type" Rotary Tool (including accessory bits: cutting, grinding, drilling, carving,
 1495 etc.)
 1496 Jeweler's screwdrivers (e.g., flat, phillips, robertson, torx, hex key)
 1497 Dentist "Type" Instruments (e.g., picks and mirrors)
 1498 Razor Saw
 1499 Small pliers (e.g., needle nose, standard nose, long nose, curved nose, side cutters)
 1500 Hammer
 1501 Chisels
 1502 Fine (small) files
 1503 Heat Gun or Heat Source
 1504 Spray Coolant
 1505 Volt-Ohm-Milliammeter (VOM) or Digital Multimeter (DMM)
 1506 Digital camera
 1507 Digital scanner

- 1508 Printer
- 1509 ANSI C Compiler
- 1510 Debugger or binary editor
- 1511 Microsoft Office Professional
- 1512 Adobe Acrobat Standard
- 1513 Miscellaneous protection equipment for chemical testing (goggles, gloves)
- 1514 Variable Power Supply
- 1515 Digital Storage Oscilloscope and/or Logic Analyzer
- 1516 Temperature Chamber

1517 7 CMVP General Testing and Reporting Guidance

1518 In order for CMVP to manage the program more efficiently, additional testing requirements are
 1519 addressed below. Several of the issues that were under section G of the FIPS 140-2
 1520 Implementation Guidance are presented in this section. This guidance does not change the
 1521 cryptographic module requirements of ISO/IEC 19790:2012 but may impact ISO/IEC
 1522 24759:2017 documentation and testing requirements.

1523 7.1 Submission Scenarios

1524 An updated version of a previously validated cryptographic module can be considered for a
 1525 *revalidation* rather than a *full validation* depending on the extent of the modifications from
 1526 the previously validated version of the module. (Note: the updated version may be, for
 1527 example, a new version of an existing cryptographic module or a new model based on an
 1528 existing model.)

1529 The [Modules In Process \(MIP\) List](#) will include only scenarios that result in issuing a new
 1530 certificate (e.g., FS, UPDT, RBND, PTSC, TRNS) if the vendor requests the entry to be
 1531 displayed on the MIP List. The Cryptographic and Security Testing Laboratories (CSTL)
 1532 must check the appropriate box in Web Cryptik for MIP List inclusion.

1533 The NIST Cost Recovery (CR) fees for all submission scenarios are posted at
 1534 [https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)
 1535 [fees](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees).

1536 Any submission that does not comply with the requirements of this section or requires
 1537 significant additional review effort by the validators (e.g., due to issues with quality or
 1538 complexity) will be subject to an ECR.

1539 Upon a satisfactory review by the CMVP, either an updated certificate or a new certificate
 1540 and an updated security policy, if there are any changes, will be posted on the [Validated](#)
 1541 [Modules](#) website.

1542 7.1.1 Requirements for all submissions

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. The CSTL is responsible for an
 1546 independent evaluation of the impacts throughout the module requirements for any change
 1547 and performs any testing needed prior to submission. The CSTL **shall** address all affected
 1548 TEs and the CSTL's assessment. The details will be included in an updated Web Cryptik
 1549 package with a summary of the changes and testing results **shall** be listed in the Change
 1550 Document (template to fill in located under the "Help" tab in Web Cryptik).

1551 For all revalidations, the Web Cryptik package **shall** include all files that are impacted by
 1552 the change with their appropriate updates (e.g., Security Policy, validation report, Draft
 1553 Certificate, and/or Physical Test Report). The ZIP file and files within the ZIP file **shall**
 1554 follow the requirements in the Web Cryptik User's Guide and submitted to the CMVP

1555 using the specified encryption methods. Additional documentation may be required if
 1556 CMVP guidance requiring the additional documentation has been published since the
 1557 module's original validation.

1558 All scenarios must be processed and submitted to the CMVP by a CSTL.

1559 If a CSTL has been contracted to perform a revalidation for a validated module for which the
 1560 CSTL did not perform the original testing on the base module:

- 1561 a. The vendor **shall** provide the CSTL with the design documentation and
 1562 implementation (including source code, HDL, etc.) of the base validated module and
 1563 of the module that has been updated.
- 1564 b. The vendor **shall** provide the CSTL with the latest Security Policy as shown on the
 1565 base module's most recent certificate.
- 1566 c. The vendor **shall** provide the CSTL with the latest validation report (a.k.a. Test
 1567 Report), if applicable per the revalidation scenario.
- 1568 d. The CSTL **shall** determine that the provided base documentation and implementation
 1569 is identical to the base validated module.
- 1570 e. The CSTL **shall** examine each modification and confirm that the change is
 1571 appropriate for the submission type (e.g., non-security relevant for Scenario NSRL).
- 1572 f. The CSTL **shall** determine that no other modifications, including unintentional, have
 1573 been made apart from what is permitted by the revalidation scenario.
- 1574 g. The CSTL **shall** meet all requirements of the revalidation scenario(s) submitted.
- 1575 h. The CSTL **shall** indicate which submission scenario is applicable and a summary of
 1576 associated changes.
- 1577 i. The CSTL **shall** use the format for listing the information for the certificate as
 1578 required by each revalidation scenario.
- 1579 j. The CSTL **shall** submit, at a minimum, what is required by the revalidation scenario.

1580 Below are the twelve possible FIPS 140-3 submission scenarios (FS, VUP, VAOE, NSRL,
 1581 ALG, OEUP, RBND, PTSC, UPDT, CVE, TRNS, PHYS). See [section 7.1.14](#) for a
 1582 summary table for these submission scenarios, and [section 7.1.15](#) for additional comments.

1583 7.1.2 Full Submission (FS)

1584 The first time a new software, firmware, hardware, or hybrid module is submitted for validation.
 1585 The module **shall** meet all applicable requirements at the time of submission.

1586 If modifications are made to hardware, software, or firmware components that do not meet any
 1587 of the below revalidation criteria, then the cryptographic module **shall** be considered a new
 1588 module and **shall** undergo a full validation testing by a CSTL and submitted as a FS.

1589 7.1.3 Vendor Update (VUP)

1590 Administrative updates (e.g., updating vendor contact information, grammatical Security Policy
 1591 corrections).

1592

1593 7.1.4 Vendor Affirmed Operational Environment (VAOE)

1594 Security policy change of vendor affirmed OEs (see Management Manual 7.9 *Vendor or User*
1595 *Affirmation of Modules*).

1596 7.1.5 Non-Security Relevant (NSRL)

1597 Modifications are made to hardware, software or firmware components **that do not affect any**
1598 **FIPS 140-3 security relevant items**. See [IG 2.4.A](#) for a definition of “security” as it relates to
1599 FIPS 140-3. The CSTL is responsible for identifying the documentation that is needed to
1600 determine whether a revalidation is sufficient, and the vendor is responsible for submitting the
1601 requested documentation to the CSTL. Documentation may include a previous validation report,
1602 design documentation, source code, source code difference evidence, FSM, security policy
1603 differences, etc.

1604 The CSTL **shall**:

- 1605 • review and independently verify the accuracy of the vendor-supplied documentation and
1606 identify any additional documentation necessary to confirm the applicability of this
1607 revalidation scenario.
- 1608 • determine additional testing as necessary to confirm that FIPS 140-3 security relevant
1609 items have not been affected by the modification.
- 1610 • identify the assertions affected by the modification and **shall** perform the tests associated
1611 with those assertions. This will require the CSTL to:
 - 1612 ○ Review the COMPLETE list of assertions applicable to the module,
 - 1613 ○ Identify, from the previous validation report, the assertions that have been
1614 affected by the modification,
 - 1615 ○ Identify additional assertions that were NOT previously tested but should now be
1616 tested due to the modification, and
 - 1617 ○ Review assertions where specific Implementation Guidance (IG) was provided at
1618 the time of the original validation to confirm that the module still meets the IG as
1619 it existed at the time of the original validation.

1620 The CSTL may send the CMVP a Request For Guidance to confirm their analysis on the non-
1621 security relevant changes prior to submission, which is expected to address at least the following
1622 questions:

- 1623 1. What changes are being proposed?
- 1624 2. What is the justification for being non-security relevant for each change?
- 1625 3. Are changes made to: approved / allowed security functions/algorithms, SSPs, approved
1626 security services, self-tests, security states within the FSM, or other areas that affects how
1627 the module meets the security objectives and requirements of FIPS 140-3?

1628 7.1.6 Algorithm Update (ALG)

1629 Post validation, approved security relevant functions or services for which CAVP testing was not
1630 available (or vendor affirming was still permitted per the CMVP/CAVP transition schedule) at
1631 the time of submission to the CMVP for validation are now CAVP-tested and are being
1632 submitted for inclusion as an approved function or service. The CSTL is responsible for
1633 identifying the documentation that is needed to determine whether a revalidation is sufficient,
1634 and the vendor is responsible for submitting the requested documentation to the CSTL.
1635 Documentation may include a previous validation report and applicable CMVP rulings, design
1636 documentation, source code, security policy differences, etc. Code or configuration changes are
1637 not permitted under this revalidation scenario. For example, if self-tests are required for
1638 approved algorithms, the module must already support these self-tests. In essence, this means
1639 that ALG can only be used when a previously vendor affirmed or allowed algorithm now has
1640 CAVP testing available and already meets the algorithm requirements (e.g., self-tests).

1641 The CSTL **shall**:

- 1642 • review and independently verify the accuracy of the vendor-supplied documentation and
1643 identify any additional documentation necessary to confirm the applicability of this
1644 revalidation scenario.
- 1645 • identify the assertions affected by the modification and **shall** perform the tests associated
1646 with those assertions. This will require the CSTL to:
 - 1647 ○ Review the COMPLETE list of assertions applicable to the module,
 - 1648 ○ Identify, from the previous validation report, the assertions that have been
1649 affected by the modification,
 - 1650 ○ Identify additional assertions that were NOT previously tested but should now be
1651 tested due to the modification, and
 - 1652 ○ Review assertions where specific Implementation Guidance (IG) was provided at
1653 the time of the original validation to confirm that the module still meets the IG as
1654 it existed at the time of the original validation, except for IGs related to the newly
1655 tested algorithm where the latest IGs **shall** be met.

1656 7.1.7 Operational Environment Update (OEUP)

1657 No changes to the module with an addition, modification, or deletion of tested operational
1658 environments (OEs). Purely deleting OEs can be done as an NSRL, but deleting can be
1659 combined in an OEUP if also adding and/or modifying OEs. This requires CAVP-testing the
1660 algorithm validations on the new/modified OEs. If an entropy source assessment is applicable
1661 per [IG 9.3.A](#), ESV(s) to cover all new/modified OEs and/or platforms **shall** be submitted and
1662 validated separately prior to submission. The CSTL **shall** perform the full regression test suite
1663 shown on the [CMVP website](#).

1664 The only time code changes are allowed as part of an OEUP is if they are non-security relevant
1665 and necessary to correctly run the module on the new/modified OE (e.g., compilation flags or
1666 configuration options that need to be updated). No other changes are permitted (even to
1667 incorporate other non-security relevant changes such as bug fixes). In this case, the CSTL

1668 selects the “Limited NSRL” sub-option in Web Cryptik after choosing the OEUP submission
1669 scenario.

1670 Upon re-testing and validation, the CMVP provides the same assurance as the original OE(s) as
1671 to the correct operation of the module on the new/modified OS(s) and/or OE(s). The
1672 new/modified OS and/or OE will be added to the module’s validation entry.

1673 As a reminder, module vendors and users may take advantage of the porting provisions
1674 explained in section 7.9.1 and 7.9.2 of this document, where performing a revalidation and
1675 updating a validation certificate may not be required.

1676 7.1.8 Rebrand (RBND)

1677 This scenario applies if there are no modifications to a module and the new module is a re-
1678 branding of an already validated Original Equipment Manufacturer (OEM) module. The CSTL
1679 **shall** include the OEM’s written approval for re-branding in the submission package and
1680 determine that the re-branded module is identical to the OEM module (n.b. this requirement
1681 applies equally to open source and non-open-source modules). Written approval **shall** note the
1682 terms of permission (e.g., subsequent addition of OEs, possible re-use of CAVP certificates,
1683 entropy, remediation of CVEs, non-security relevant changes, whether a rebrand of a rebrand is
1684 acceptable, etc.). If these terms do not explicitly allow a vendor to further rebrand the OEM
1685 module, then a rebrand of that rebranded module is not permitted unless written permission is
1686 granted by the OEM. Additionally, for modules containing any open-source licensed code, the
1687 CSTL **shall** ensure the open-source licensing requirements are met (e.g., any required notices are
1688 contained in the Security Policy). The submission **shall** include a letter requesting the validation
1689 of the re-branded module and indicate the applicable documentation changes (e.g., vendor name,
1690 address, POC information, versioning information, etc.).

1691 A RBND **shall** include at least one OE from the original validation and cannot include OEs that
1692 are not listed in the original validation. With proper OEM permissions, an RBND followed by an
1693 OEUP can accomplish rebranding a module on different OEs. CAVP testing **shall** cover all of
1694 the list OEs.

1695 The only time it is allowed to combine a RBND with other scenarios is as follows:

1696 a. A RBND may be combined with a PHYS only if physical changes are necessary to
1697 correctly rebrand the module. For example, if the paint or coating on the hardware of the
1698 rebranded module is changed to reflect the new company’s color schemes, and/or to
1699 change the vendor and product names on the enclosure. In this case, the CSTL selects the
1700 “PHYS” sub-option in Web Cryptik after choosing the RBND submission scenario.

1701
1702 b. The only time code changes are allowed as part of a RBND is if they are necessary to
1703 correctly rebrand the module (e.g., to display the new module name/version/logo, or to
1704 use the new vendor’s color schemes/visual aesthetics). No other changes are permitted
1705 (even to incorporate other non-security relevant changes such as bug fixes). In this case,
1706 the CSTL selects the “Limited NSRL” sub-option in Web Cryptik after choosing the
1707 RBND submission scenario.

1708
1709 c. A vendor may reuse OEM’s CAVP certificates with proper permission. But if the OEM

1710 does not permit the vendor to reuse the CAVP certificates, then the vendor will need to
 1711 perform CAVP testing on all listed OEs. If CAVP testing is redone, the CSTL selects the
 1712 “CAVP Testing Redone” sub-option in Web Cryptik after choosing the RBND
 1713 submission scenario.

1714
 1715 d. A RBND is almost guaranteed to be combined with a VUP to address the vendor changes
 1716 so this will not be separately selectable in Web Cryptik.

1717 The CSTL **shall** provide an updated security policy which is technically identical to the
 1718 originally validated security policy and describes the re-branded module.

1719 7.1.9 Port Sub Chip (PTSC)

1720 A sub-chip cryptographic subsystem that was previously validated in a single-chip (see [IG 2.3.B](#))
 1721 can be ported to other single-chip constructs as a PTSC submission to the CMVP. The following
 1722 is applicable to validate this new single-chip module:

- 1723 • The CSTL **shall** verify that there are no security relevant changes in the sub-chip
 1724 cryptographic subsystem;
- 1725 • If an entropy source is contained within the sub-chip cryptographic subsystem, ESV(s) to
 1726 cover all new single-chip environments **shall** be submitted and validated separately prior
 1727 to submission;

1728 **Note 1:** An ESV may not be required, if the entropy is collected outside the sub-chip
 1729 cryptographic subsystem, depending on changes to the entropy source or the
 1730 subsystem housing it. Please refer to [IG 9.3.A](#) and [IG D.J](#) for details on applicable
 1731 caveats and entropy estimates.

1732 **Note 2:** Single chip embodiments may implement an ESV or a DRBG linked to a dedicated
 1733 entropy source inside the physical boundary. Such cases may be implemented (a)
 1734 inside the sub-chip cryptographic subsystem or (b) in two or more sub-chip
 1735 cryptographic subsystems. The case (b) represents multiple disjoint sub-chip
 1736 cryptographic subsystems (see 3 of [IG 2.3.B](#)).

- 1737 • Approved security functions **shall** be retested and validated by the CAVP if implemented
 1738 in a soft circuitry core recompiled in a different part configuration. In this case, the CSTL
 1739 selects the “CAVP Testing Redone” sub-option in Web Cryptik after choosing the PTSC
 1740 submission scenario.

1741 **Note 3:** If the original algorithm testing was performed as stated in the [Management Manual](#)
 1742 Section 7.3 – *Testing using Emulators and Simulators* in a module simulator, and there is
 1743 no change to the soft-core, no additional algorithm testing is required.

- 1744 • Full regression testing (see FIPS 140-3 [Resources page](#)) **shall** be performed on the new
 1745 sub-chip cryptographic subsystem after fabrication (transformation of the HDL to a gate
 1746 or physical circuitry representation);
- 1747 • **ISO/IEC 19790:2012** Section 7.3 **shall** be addressed for the new single-chip module for
 1748 all Security Levels within this Section.
- 1749 • **ISO/IEC 19790:2012** Section 7.7 **shall** be addressed for the new single-chip module at
 1750 Security Level 1.

- 1751 • **ISO/IEC 19790:2012** Sections 7.11.2 and 7.11.9 **shall** be addressed for the new single-
 1752 chip module for all Security Levels within this Section.
- 1753 • A new Security Policy **shall** be provided for the new single-chip module.
- 1754 • Versioning information on the new certificate **shall** be provided for:
- 1755 ○ the new physical single-chip,
- 1756 ○ non-security relevant single-chip functional subsystem firmware if applicable,
- 1757 ○ the sub-chip cryptographic subsystem soft and hard circuitry cores (which are
 1758 unchanged from the original validation), and
- 1759 ○ the associated firmware.
- 1760 • The only time code changes are allowed as part of an PTSC is if they are non-security
 1761 relevant and necessary to correctly run the module on the new/modified single chip
 1762 environment (e.g., compilation flags or configuration options that need to be updated).
 1763 No other changes are permitted (even to incorporate other non-security relevant changes
 1764 such as bug fixes). In this case, the CSTL selects the “Limited NSRL” sub-option in
 1765 Web Cryptik after choosing the PTSC submission scenario.

1766 7.1.10 Update (UPDT)

1767 Modifications are made to hardware, software or firmware components **that affect some of the**
 1768 **FIPS 140-3 security relevant items**. See [IG 2.4.A](#) for a definition of “security” as it relates to
 1769 FIPS 140-3. An updated cryptographic module can be considered in this scenario if less than a
 1770 30% of security changes were made to the module. Security changes include impacts to:
 1771 approved / allowed security functions/algorithms, SSPs, approved security services, self-tests,
 1772 and security states within the FSM. None of these, assessed individually, can exceed 30% of
 1773 changes. The individual ratios for each of these **shall** be provided to the CMVP within the
 1774 Change Document (e.g., 2 approved security services out of 10 total results in 20% change).

1775 The CSTL is responsible for identifying the documentation that is needed to determine whether a
 1776 revalidation is sufficient, and the vendor is responsible for submitting the requested
 1777 documentation to the CSTL. Documentation may include a previous validation report and
 1778 applicable CMVP rulings, design documentation, source code, source code difference evidence,
 1779 FSM etc.

1780 The CSTL **shall**:

- 1781 • provide a summary of the changes and rationale of why this meets the <30% guideline.
 1782 The CMVP upon review, may determine that the changes are >30% and **shall** be
 1783 submitted as an FS.
- 1784 • review and independently verify the accuracy of the vendor-supplied documentation and
 1785 identify any additional documentation necessary to confirm the applicability of this
 1786 revalidation scenario.
- 1787 • identify the assertions affected by the modification and **shall** perform the tests associated
 1788 with those assertions. This will require the CSTL to:
- 1789 ○ Review the COMPLETE list of assertions applicable to the module,
- 1790 ○ Identify, from the previous validation report, the assertions that have been
 1791 affected by the modification,

- 1792 ○ Identify additional assertions that were NOT previously tested but should now be
1793 tested due to the modification, and
- 1794 ○ Review assertions where specific Implementation Guidance (IG) was provided to
1795 confirm that the module meets all current applicable IGs.

1796 In addition to the tests performed against the affected assertions, the CSTL **shall** perform the
1797 regression test suite shown on the [CMVP website](#).

1798 The UPDT can also be used to for resetting the module’s sunset date when a module has not
1799 changed, provided the above requirements are met.

1800 UPDT can be combined with any submission scenario(s) except VUP or VAOE. In this case, the
1801 CSTL selects the appropriate sub-option(s) in Web Cryptik after choosing the UPDT submission
1802 scenario.

1803 7.1.11 Common Vulnerabilities and Exposures (CVE)

1804 A CSTL has been contracted to perform a revalidation for a module on which the vendor has
1805 made FIPS 140 security-relevant changes in response to one or more CVEs (Common
1806 Vulnerability and Exposure). For more information about CVEs please see
1807 <https://cve.mitre.org/>.

1808 The purpose of this revalidation scenario is to provide the vendor a means to quickly fix, test and
1809 revalidate a module that is subject to a *security-relevant CVE*¹, while at the same time providing
1810 assurance that the module still meets the FIPS 140-3 standard. If a CVE does not require
1811 security relevant changes to address it, then the vendor may pursue a Scenario NSRL
1812 revalidation.

1813 To complete a Scenario CVE revalidation:

- 1814 a. The CSTL **shall** determine that security relevant changes to the module are only
1815 to correct the vulnerability disclosed in the CVE. Other changes are permitted if
1816 only directly impacted by the CVE change (e.g., addressing the CVE may require
1817 changing the version number, and that requires the show version service be
1818 updated). In this case, the CSTL selects the “Limited NSRL” sub-option in Web
1819 Cryptik after choosing the CVE submission scenario.
- 1820 b. The CSTL **shall** examine each modification and confirm that the change does not
1821 conflict with the requirements of FIPS 140-3.
- 1822 c. The CSTL **shall** determine that no other modifications have been made.
- 1823 d. The CSTL **shall** identify the assertions affected by the security-relevant
1824 modification and **shall** perform the tests associated with those assertions.
- 1825 e. The vendor is not required to address IGs that have been published since
1826 submission of the original module, besides following the continual guidance of [IG](#)
1827 [11.A](#) (CVE Management).
- 1828 f. If the fix to address the CVE is in the scope of an algorithm implementation (e.g.,
1829 involves a change that requires retesting per the CAVP), then this algorithm **shall**
1830 be CAVP tested again to obtain a new CAVP certificate with the new module

1831 version. In this case, the CSTL selects the “CAVP Testing Redone” sub-option in
1832 Web Cryptik after choosing the CVE submission scenario.

1833 In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the
1834 predefined regression tests shown on the [CMVP website](#), under CVE.

1835 Because the change to the module is to address a security-relevant CVE, **the previous version of**
1836 **the module is no longer considered validated and shall be removed from the certificate;**
1837 exceptions may be made if the vendor shows how the CVE can be mitigated by policies included
1838 in the Security Policy, while still adhering to the FIPS 140-3 standard.

1839 ¹ A *security-relevant CVE* is one that affects how the module meets the requirements of the FIPS
1840 140-3 standard.

1841 7.1.12 Algorithm Transition (TRNS)

1842 A CSTL has been contracted to perform a revalidation for a module on which the vendor has
1843 made FIPS 140-3 security relevant changes solely in response to a published CMVP algorithm
1844 transition that will cause some previously validated modules to be placed on the Historical list.
1845 If the algorithm transition will NOT cause the module to move to the historical list (i.e., “soft”
1846 transition), changes cannot be made as part of this submission. For example, the non-SP 800-
1847 56Brev2 RSA-based key encapsulation/un-encapsulation transition explained in FIPS 140-3 [IG](#)
1848 [D.G.](#)

1849 Note: a single Scenario TRNS submission may combine multiple algorithm transitions.
1850 However, this may increase review time.

1851 The purpose of the TRNS revalidation is to provide the vendor a means to quickly address
1852 algorithm transition requirements, test and revalidate a module in order to meet a CMVP
1853 transition, while at the same time providing assurance that the module still meets the FIPS 140-3
1854 standard.

1855 If the module code is *changed* to address an algorithm transition, the following requirements
1856 apply:

- 1857 a. Submitted as a Scenario TRNS.
- 1858 b. The CSTL **shall** determine that security relevant changes to the module are only
1859 to address a specific CMVP transition. Other changes are permitted if only
1860 directly impacted by the TRNS change (e.g., addressing the TRNS may require
1861 changing the version number, and that requires the show version service be
1862 updated). In this case, the CSTL selects the “Limited NSRL” sub-option in Web
1863 Cryptik after choosing the TRNS submission scenario.
- 1864 c. The CSTL **shall** examine each modification and confirm that the change does not
1865 conflict with the requirements of FIPS 140-3.
- 1866 d. The CSTL **shall** determine that no other modifications have been made. The
1867 vendor is not required to address IGs or guidance that have been published since
1868 submission of the original module, unless directly applicable to the transitioning
1869 algorithm (e.g., CAVP testing or self-test requirements).

- 1870 e. The CSTL **shall** identify the assertions affected by the security-relevant
 1871 modification and **shall** perform the tests associated with those assertions.
 1872 f. If the means to meet the transition are in the scope of an algorithm
 1873 implementation, and the path chosen to meet the requirements necessitates testing,
 1874 then this algorithm **shall** be CAVP tested to obtain a new CAVP certificate with
 1875 the new module version. In this case, the CSTL selects the “CAVP Testing
 1876 Redone” sub-option in Web Cryptik after choosing the TRNS submission
 1877 scenario.
 1878 g. In addition to the tests performed against the affected assertions, the CSTL **shall**
 1879 also perform the predefined regression tests shown on the [CMVP website](#) under
 1880 “TRNS – Code Change” on all versions listed on the module’s certificate and on
 1881 at least one of the listed OEs for hybrid or software/firmware modules (if the
 1882 module binary image is identical across all OEs; if not, testing on at least every
 1883 binary image is required).
 1884 h. The CSTL **shall** provide justification on why regression testing is not necessary
 1885 for the untested OEs. With proper justification, these may remain on the
 1886 module’s certificate.
 1887 i. If regression testing is not performed on some versions, then those **shall** be
 1888 removed from the module’s certificate. OEs without proper justification or
 1889 regression testing **shall** be removed from the module’s certificate.

1890 If the module code is *unchanged* to address an algorithm transition and the change is purely to
 1891 documentation, one of the following four options apply. For each option, the CSTL **shall** state
 1892 that the change to address the transition is purely documentational and which option applies.

1893 **Option 1:** services or functionality were not moved to or from an approved mode to remain
 1894 compliant (e.g., previously non-compliant services remain in an approved mode but are updated
 1895 to demonstrate compliance rather than moved into a non-approved mode), then the vendor may
 1896 pursue a Scenario ALG revalidation.

1897 **Option 2:** The vendor moves all non-compliant functionality into a non-approved mode of
 1898 operation from an approved mode of operation.

- 1899 a. Submitted as a Scenario TRNS.
 1900 b. The CSTL **shall** determine that security relevant changes to the module are only
 1901 to address a specific CMVP transition.
 1902 c. The CSTL **shall** examine each modification and confirm that the change does not
 1903 conflict with the requirements of FIPS 140-3.
 1904 d. The CSTL **shall** determine that no other modifications have been made. The
 1905 vendor is not required to address IGs or guidance that have been published since
 1906 submission of the original module, unless directly applicable to the transitioning
 1907 algorithm (e.g., CAVP testing or self-test requirements).

- 1908 e. The CSTL **shall** identify the assertions affected by the security-relevant
 1909 documentation modification and **shall** perform the tests associated with those
 1910 assertions.
 1911 f. The CSTL **shall** demonstrate how the module still meets [IG 2.4.C](#) after the
 1912 reclassification of non-compliant functionality into a non-approved mode of
 1913 operation.
 1914 g. In addition to the tests performed against the affected assertions, the CSTL **shall**
 1915 also perform the predefined regression tests shown on the [CMVP website](#) under
 1916 “TRNS - No Code Change” on all versions listed on the module’s certificate and
 1917 on at least one of the listed OEs for hybrid or software/firmware modules (if the
 1918 module binary image is identical across all OEs; if not, testing on at least every
 1919 binary image is required).

1920 The only exception to this requirement (g.) is if the algorithm being transitioned is
 1921 part of a standalone service and is not used by any other module service (e.g.,
 1922 cryptographic library where the module only provides the algorithm as an API
 1923 service to a calling application as a stand-alone service). In this case, the CSTL
 1924 **shall** provide justification on why regression testing is not necessary at all.

- 1925 j. The CSTL **shall** provide justification on why regression testing is not necessary
 1926 for the untested OEs. With proper justification, these may remain on the
 1927 module’s certificate.
 1928 k. If regression testing is not performed on some versions, then those **shall** be
 1929 removed from the module’s certificate. OEs without proper justification or
 1930 regression testing **shall** be removed from the module’s certificate.
 1931 h. The CSTL **shall** provide assurance that the non-compliant functionality is not
 1932 used to meet any FIPS 140-3 requirements (key/CSP establishment, generation,
 1933 storage, etc.).
 1934 i. The CSTL **shall** provide assurance, upon module examination, that no service,
 1935 algorithm or CSP that relied on or used the non-compliant functionality,
 1936 parameters, keys, etc. remain in an approved mode. An approved mode **shall**
 1937 only contain approved services.
 1938 j. Documentation **shall** be updated to indicate the module does not utilize non-
 1939 compliant functionality in an approved mode of operation.

1940 **Option 3:** The vendor recategorizes the non-compliant functionality as claiming no security per
 1941 [IG 2.4.A](#), and this functionality remains in an approved mode of operation.

- 1942 a. The same rules for Option 2 above **shall** be followed except for bullets ‘i’ and ‘j’.
 1943 b. The CSTL **shall** provide justification on how the requirements of [IG 2.4.A](#) are
 1944 met. This scenario is intended to be rarely used/accepted and depends on the
 1945 purpose or use of the service that utilizes the non-approved algorithms. For
 1946 example, a software library implementing three-key Triple-DES Encryption as
 1947 one of its approved services cannot simply state this algorithm does not claim any

1948 security (per [IG 2.4.A](#)) and be used in an approved mode, as this does not meet 3)
1949 or 4) in [IG 2.4.A](#) Additional Comment #2.

1950 **Option 4:** A combination of any of three options above (CAVP testing, moving non-compliant
1951 functionality into the a non-approved mode, and/or recategorized per [IG 2.4.A](#)), in which case,
1952 requirements of each option apply.

- 1953 a. Submitted as a Scenario TRNS.
1954 b. Each option **shall** be listed/indicated in the Change Document under Option 4
1955 (e.g. under Option 4, the following are claimed: Options 1 and 2) and note how
1956 each of the applicable ‘shall’ statements for each option are met).

1957 In order to accommodate vendors who are updating their validation to prepare for an algorithm
1958 transition, fully compliant TRNS or ALG revalidations that have addressed the transition and are
1959 submitted to the CMVP before the date the transition is to take effect, will remain on the active
1960 list through the completion of the revalidation, even if it is not completed until after the transition
1961 date, unless the algorithm transition is to address a security concern that is deemed unacceptable
1962 by the CMVP. For newly submitted ALG submissions that address the transition, the CSTL
1963 **shall** include in the Special Instructions field the text “algorithm_transition” (with or without the
1964 underscore) in order for the CMVP not to move this submission to the historical list come the
1965 algorithm transition date.

1966 Changes made to a module, whether to the module code or purely to documentation, in order to
1967 meet a transition are security-relevant, due to their potential impacts on core and downstream
1968 services and the treatment of keys and SSPs. For example, moving *allowed* functionality from
1969 an approved mode to a non-approved mode - by either changing the software/firmware or a
1970 purely documentation change - is considered security relevant. Therefore, besides the case in
1971 **Option 1** above, all submissions that address a transition will require a Scenario UPDT, TRNS
1972 or FS submission regardless of module type or security level.

1973 If a Scenario TRNS revalidation addresses an algorithm transition that moved the original
1974 certificate to the Historical list, and the sunset date of the certificate has yet to expire, then upon
1975 the revalidation of the module under Scenario TRNS, a new certificate will be issued on the
1976 Active list (inheriting the original sunset date) for the version of the module compliant with the
1977 transition requirements. Otherwise, if the original certificate was moved to the Historical list for
1978 reasons that are not addressed in the TRNS revalidation (e.g., a separate algorithm transition or
1979 the sunset date expired), the new certificate will be shown on the Historical list *immediately* after
1980 completion of the TRNS revalidation.

1981 7.1.13 Physical Enclosure (PHYS)

1982 Modifications are made only **to the physical enclosure of the cryptographic module that**
1983 **provides its protection and involves no operational changes to the module.** The CSTL is
1984 responsible for ensuring that the change only affects the physical enclosure (integrity) and has no
1985 operational impact on the module. The CSTL **shall** fully test the physical security features of the
1986 new enclosure to ensure its compliance to the applicable requirements of the standard.

1987 The CSTL **shall**:

- 1988 a. Describe the change (pictures may be required),
- 1989 b. State that it is a security relevant change,
- 1990 c. Provide sufficient information supporting that the physical only change has no
- 1991 operational impact,
- 1992 d. Describe the tests performed by the CSTL that confirm that the modified enclosure still
- 1993 provides the same physical protection attributes as the previously validated module. For
- 1994 physical security levels 2, 3 and 4, the CSTL **shall** submit an updated Physical Security
- 1995 Test Report.

1996 7.1.14 Submission Scenario Summary Table

Scenario	Long Name	<u>A</u> ctive or <u>H</u> istorical ¹	New or Updated Cert ²	New Sunset Date ³	Meet All Latest Guidance ⁴	Entropy Testing Applicable (ESV) ⁵	ENT Remain on Cert ⁷	Predefined Regression Testing ⁸
VUP	Vendor Update	A or H	Updated	No	No	No	Possible	No (nor optional testing)
VAOE	Vendor Affirmed Operational Environment	A or H	Updated	No	No	No	Possible	No (nor optional testing)
NSRL	Non-Security Relevant	A only	Updated	No	No	No	Possible	No
ALG	Algorithm Update	A only	Updated	No	No (except for the algorithm updated)	No	Possible	No
OEUP	Operational Environment Update	A only	Updated	No	No	Yes ⁶	Possible	Yes (full regression table)
RBND	Rebrand	A only	New	No	No	No	Possible	No (nor optional testing)
PTSC	Port Sub Chip	A only	New	No	No	Yes ⁶	Possible	Yes (full regression table)
UPDT	Update	A or H	New	Yes	Yes	Yes	No	Yes (full regression table)
CVE	Common Vulnerabilities and Exposures	A or H	Updated	No	No	No	Possible	Yes (subset of regression table)
TRNS	Algorithm Transition	A or H	New	No	No (except for the algorithm transitioning)	No	Possible	Yes (subset of regression table)
PHYS	Physical Enclosure	A only	Updated	No	No	No	Possible	Yes (physical security)
FS	Full Submission	N/A	New	Yes	Yes	Yes	No	Full testing

1997 ¹ A or H means the revalidation can be on a completed validation that is either Active *or* Historical; A
 1998 only means it can only be on an Active validation.

1999 ² The result of this validation or revalidation will either be a new certificate (new number) or an updated
 2000 certificate (same number).

2001 ³ The result of this validation or revalidation will either be a new sunset date of 5 years, or the sunset date
 2002 will remain the same. See Additional Comment #3 below for more details.

2003 ⁴ If Yes, the validation or revalidation **shall** meet all the latest applicable guidance and requirements (e.g.,
 2004 standards, implementation guidance, management manual guidance, algorithm testing/self-tests, and other
 2005 CMVP guidance) at the time of submission to the CMVP unless there is an implementation guidance
 2006 transition that affects reports in the queue. If No, the revalidation **shall** meet all applicable requirements
 2007 at the time of *original* validation (a module does not need to meet requirements that were added since the
 2008 time of original validation, except those specified in the table).

2009 ⁵ If applicable per [IG 9.3.A](#).

2010 ⁶ Only required on the new OEs for OEUP, or new single-chip environments for PTSC.

2011 ⁷ Only for the original validation’s ENT claim. No new ENT claims are possible, for any validation or
 2012 revalidation.

2013 ⁸ Note: additional regression testing (on top of the predefined ones) may be applicable per requirements of
 2014 the scenario. See the [CMVP FIPS 140-3 Resources](#) page for the pre-defined regression tests.

2015 7.1.15 Additional Comments

2016 1. If the overall Security Level of the cryptographic module is lowered or remains the
 2017 same, the module may be submitted as a UPDT with full testing on the individual
 2018 section(s) that is being lowered.

2019 2. If the overall Security Level of the cryptographic module is raised or if the physical
 2020 embodiment changes, e.g., from multi-chip standalone to multi-chip embedded, then
 2021 the cryptographic module will be considered a new module and **shall** undergo full
 2022 validation testing by a CSTL and submitted as an FS.

2023 3. The sunset date for the module is determined based on the scenario:

- 2024 ● Scenarios FS, UPDT – sunset date will be 5 years from the validation date
- 2025 ● Scenarios VUP, VAOE, NSRL, ALG, OEUP, CVE, PHYS – sunset date unchanged
- 2026 ● Scenarios RBND, PTSC, TRNS – sunset date is inherited from the original
 2027 certificate

2028 4. It is **not** possible to combine any revalidation scenarios outside of what is explicitly
 2029 permitted by the submission scenario. For example, if a vendor would like to rebrand
 2030 (RBND) a PTSC submission, this would need to happen in two separate submissions (i.e.,
 2031 RBND followed by a PTSC). Similarly, despite it being a simple change, a VU or VAOE
 2032 would need to be submitted separately to address any vendor admin change or vendor
 2033 affirmed OE changes, respectfully, and cannot be combined with other scenarios. This will

2034 give the CMVP the most flexibility to address each scenario submission effectively and
 2035 efficiently.

2036 A summary table of the permitted combinations are below:

		Added/secondary scenario										
		VUP	VAOE	NSRL	ALG	OEUP	RBND	PTSC	UPDT	CVE	TRNS	PHYS
Main Submission	VUP	-	-	-	-	-	-	-	-	-	-	-
	VAOE	-	-	-	-	-	-	-	-	-	-	-
	NSRL	-	-	-	-	-	-	-	-	-	-	-
	ALG	-	-	-	-	-	-	-	-	-	-	-
	OEUP	-	-	✓	✓	-	-	-	-	-	-	-
	RBND	✓	-	✓	✓	-	-	-	-	-	-	✓
	PTSC	-	-	✓	✓	-	-	-	-	-	-	-
	UPDT	-	-	✓	✓	✓	✓	✓	✓	-	✓	✓
	CVE	-	-	✓	✓	-	-	-	-	-	-	-
	TRNS	-	-	✓	✓	-	-	-	-	-	-	-
	PHYS	-	-	-	-	-	-	-	-	-	-	-

2037 ✓ - The Added/secondary scenario will NOT be separately selectable as a sub-option in
 2038 WebCryptik (e.g., VUP changes will always be possible under a RBND).

2039 ✓ - The Added/secondary scenario WILL be separately selectable as a sub-option. The
 2040 Added/secondary scenario may be further locked down / limited per the Main Submission
 2041 definition (e.g., NSRL changes associated with an OEUP submission must be specific to running
 2042 the new OEs, rather than permitting *any* NSRL changes).
 2043

2044 For the revalidation scenarios that *can* be combined (i.e., red checkbox in the table above),
 2045 the main submission **shall** meet all applicable requirements of the added/security scenario,
 2046 in addition to the main scenario requirements. For example, a RBND + NSRL must include
 2047 proper regression testing and documenting the changes per NSRL specifications.

2048 5. A revalidation submission cannot be performed on a submission that is in the queue. It
 2049 **shall** be on a completed validation (e.g., UPDT on a *validated* FS).

2050 **7.2 CMVP requirements pertaining to testing and approved algorithms**

2051 FIPS 140-3 describes approved security functions which can be used in an approved mode of
 2052 operation, and non-approved security functions which cannot be used in an approved mode of
 2053 operation. Approved security functions are expected to be CAVP tested, but CAVP testing has
 2054 not always been available for these methods.

2055 In such cases where CAVP testing is not available, guidance must be written to permit using
 2056 these algorithms in an approved mode. These algorithms may be “vendor affirmed” to meet the
 2057 applicable standard(s).

2058 In addition, security methods that fall outside of the list of approved methods cannot be used in
 2059 an approved mode, unless guidance is written to permit such special cases, where these methods
 2060 are *allowed* to be used in the approved mode of operation; or as permitted under AS02.21.

2061 This section explains when vendor affirmed or *allowed* methods are permitted, as well as the
 2062 transitioning from vendor affirmed to CAVP Testing.

2063 7.2.1 Vendor Affirmation of Security Functions and Methods

2064 If CAVP testing is not available or the module is submitted during a transition period, then the
 2065 following guidance is applicable.

2066 If new approved methods (e.g., NIST FIPS, SP, etc.) are added to SP 800-140 documents, until
 2067 such time that CAVP testing is available or the transition period has not yet expired for the new
 2068 method, the CMVP will:

- 2069 ○ if applicable, allow methods as provided by existing guidance (untested, and listed as
 2070 non-approved but *allowed* in an approved mode as shown in IGs [D.F](#) and [D.G](#)); and
- 2071 ○ permit the vendor to implement the new approved method if an IG that supports
 2072 vendor affirmation of this algorithm is published and met (untested, listed as
 2073 approved for use in an approved mode with the caveat “vendor affirmed”).

2074 Note:

- 2075 1. The Cryptographic Technology Group (CTG) at NIST may determine prior methods may be
 2076 retroactively disallowed and moved to non-approved and not permitted in an approved mode
 2077 of operation (e.g., DES). A transition notice would appear in NIST publications.
- 2078 2. For all approved methods, all applicable FIPS 140-3 requirements **shall** be met. An IG may
 2079 further clarify the requirements for a vendor affirmed algorithm.

2080 Additional Comments

2081 **Vendor Affirmed:** a security method reference that is listed with this caveat has not been tested
 2082 by the CAVP, and the CMVP or CAVP provide no assurance regarding its correct
 2083 implementation or operation. Only the vendor of the module affirms that the method or
 2084 algorithm was implemented correctly.

2085 The users of cryptographic modules implementing vendor affirmed security functions must
 2086 consider the risks associated with the use of untested and unvalidated security functions.

2087 7.2.2 Transitioning from vendor affirmed to CAVP Testing

2088 When CAVP algorithm testing is released on the ACVTS production server in any of the
 2089 following 3-month periods identified below, the transition occurs at the end of the following 3-
 2090 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

2091 *Table 1 - CAVP testing release dates and subsequent CMVP Transition dates*

2092 To illustrate, if the CAVP releases new testing for algorithm A, B and C, during the July 1 –
 2093 September 30 period, then the transition date will be September 30 + three months, so after
 2094 December 31 vendor affirming to algorithms A, B, or C will be prohibited in initial report
 2095 submissions.

2096 During the transition period, a new approved method would either be listed as approved with a
 2097 reference to a CAVP validation certificate, or as vendor affirmed if testing was not performed
 2098 and an IG that supports vendor affirmation of this algorithm was met.

2099 When the transition period ends, for newly received test reports:

- 2100 ○ only approved methods that have been tested, receives a CAVP validation certificate
 2101 and is verified to meet the underlying algorithm standard is permitted. All other
 2102 methods would be listed as non-approved and not allowed in an approved mode of
 2103 operation.
- 2104 ○ the vendor could optionally follow up with testing of untested vendor affirmed methods
 2105 and if so, the reference to vendor affirmed would be removed and replaced by reference
 2106 to the algorithm certificate. If there are no changes to the module, this change can be
 2107 submitted under Scenario ALG (see Section 7.1 – *Submission Scenarios*). If the
 2108 module is changed, this can be submitted under Scenarios UPDT or FS as applicable.

2109 **Note:** To track the algorithms and their transition dates, the CMVP maintains a table available on
 2110 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions)
 2111 [transitions](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions)).

2112 **Note:** If a self-test requirement is associated with the algorithm, the algorithm will only be
 2113 considered as an approved algorithm by CMVP if the self-test requirement is also met.

2114 7.3 Testing using Emulators and Simulators

2115 Under certain circumstances it may not be possible to test a module or algorithm directly. In
 2116 these cases, CMVP has permitted the use of emulators and simulators to model the behavior of

2117 the item being tested. It is important to note the differences of these models and to apply them
2118 under the correct circumstances.

2119 An emulator attempts to “model” or “mimic” the behavior of a cryptographic module. The
2120 correctness of the emulators' behavior is dependent on the inputs to the emulator and how the
2121 emulator was designed. It is not guaranteed that the actual behavior of the cryptographic module
2122 is identical, as other variables may not be modeled correctly or with certainty.

2123 A simulator exercises the actual source code (e.g., Very High-Speed Integrated Circuit (VHSIC)
2124 Hardware Description Language (VHDL) code) prior to physical entry into the module (e.g., a
2125 Field-Programmable Gate Array (FPGA) or custom Application-Specific Integrated Circuit
2126 (ASIC)). From a behavioral perspective, the behavior of the source code within the simulator
2127 may be logically identical when placed into the module or instantiated into logic gates. However,
2128 many other variables exist that may alter the actual behavior (e.g., path delays, transformation
2129 errors, noise, environmental, etc.). It is not guaranteed that the actual behavior of the
2130 cryptographic module is identical, as many other variables may not be identified with certainty.

2131 Labs may apply emulators or simulators depending on the type of testing results to be achieved.
2132 There are three broad areas of focus during the testing of a cryptographic module: operational
2133 testing of the module at the defined boundary of the module, algorithm testing and operational
2134 fault induction testing.

- 2135 1. Operational Testing – Emulation or simulation is prohibited for the operational testing of a
2136 cryptographic module. Actual testing of the cryptographic module must be performed
2137 utilizing the defined ports and interfaces and services that a module provides. A test
2138 harness or a modified version to induce an error may be utilized; however, no changes to
2139 code or circuitry responsible for the tested response may be made.
- 2140 2. Operational Fault Induction – An emulator or simulator may be utilized for fault induction
2141 to test a cryptographic module’s transition to error states as a complement to the source
2142 code review. Rationale must be provided for the applicable TE as to why a method does
2143 not exist to induce the actual module into the error state for testing.
- 2144 3. Algorithm Testing – Algorithm testing utilizing the defined ports and interfaces and
2145 services that a module provides is the preferred method. This method most clearly meets
2146 the requirements of [IG 2.3.A](#). If this preferred method is not possible where the module’s
2147 defined set of ports and interfaces and services do not allow access to internal algorithmic
2148 engines, two alternative methods may be utilized:
 - 2149 a. A module may be modified under the supervision of the CSTL for testing purposes
2150 to allow access to the algorithmic engines (e.g., test jig, test API), or
 - 2151 b. A module simulator may be utilized.

2152 When submitting the algorithm test results to the CAVP, the actual OE on which the testing was
2153 performed must be specified (e.g., including modified module identification or simulation
2154 environment). When submitting the module test report to the CMVP, AS2.20 must include
2155 rationale explaining why the algorithm testing was not conducted on the actual cryptographic
2156 module. An emulator may not be used for algorithm testing.

2157 7.4 Remote Testing of Modules

2158 The guidance below addresses the need for testing a module remotely while obtaining the
 2159 equivalent assurance as if the test were performed at the **vendor's facility**. All physical security
 2160 testing except for Environment failure protection/testing (i.e., EFT/EPT tests: TE.07.73.01,
 2161 TE.07.77.01-03 and TE.07.81.01-02) **shall** be performed in person by a CSTL tester at either the
 2162 vendor, the CSTL site and/or remote site as per HB 150-17 requirements.

2163 The CSTL may perform some or all testing remotely. If the testing is performed remotely at the
 2164 vendor site, the following conditions **shall** be met:

- 2165 1. a. The hardware, firmware or hybrid IUT is located at the vendor site.
- 2166 b. The software IUT is located at the vendor site or 3rd party cloud system.
- 2167 2. The vendor remotely provides a cryptographic module to the test laboratory and its
 2168 boundary and version are verified against the Security Policy. (ISO/IEC 24759
 2169 TE04.13.01, 02, 03). The module boundary and version **shall** be verified at the beginning
 2170 of any new remote testing sessions.
- 2171 3. a. The network access and/or video conference to a remote test operational environment,
 2172 in support of actual testing, **shall** be authorized and controlled by the vendor.
- 2173 b. A 3rd party cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google
 2174 Cloud) may be used as a service in support of module validation (e.g. video conference
 2175 and data storage) if:
 - 2176 • all HB 150-17 and NVLAP General Criteria Checklist ISO_IEC 17025
 2177 requirements are met; and
 - 2178 • the remote testing requirements are met.
- 2179 c. A cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google Cloud)
 2180 may be used as a testing platform if:
 - 2181 • all HB 150-17 and NVLAP General Criteria Checklist ISO_IEC 17025
 2182 requirements are met;
 - 2183 • the remote testing requirements are met;
 - 2184 • the environment provides the same level or additional level of security as
 2185 the lab would provide for internal testing;
 - 2186 • the cryptographic module under test **shall** be confirmed to be running on
 2187 an OE that is well-defined and has a specific OS version, hardware
 2188 platform and version, and processor (including microprocessor version) as
 2189 shown on the module's certificate and security policy; and
 - 2190 • the OS version, hardware platform and version, and processor **shall** be
 2191 confirmed during the testing session.

- 2192 d. As permitted within a signed agreement by the lab and vendor:
- 2193 • The tester's network **shall** be connected to the vendor's network via a
- 2194 secure connection (e.g., VPN or SSH) ; and/or
- 2195 • A secure video conference **shall** be used and the recording done in a
- 2196 secure manner.
- 2197
- 2198 e. The tester's tools must satisfy the lab's network requirements before connecting to the
- 2199 vendor's network to test the module if applicable.
- 2200 4. The CSTL **shall** have a procedure for conducting remote testing at the vendor site which
- 2201 includes the following:
- 2202 a. All the remote testing sessions that produce the final test results **shall** be recorded and
- 2203 archived at the CSTL as evidence material to demonstrate the tester control and/or
- 2204 oversight (as per bullet 6 below) (e.g. video conference records and/or detailed test plan)
- 2205 and to capture the test results (e.g. video conference records, screenshots and/or log files).
- 2206 b. If multiple remote testing sessions are required, a log which includes the date and the
- 2207 test being conducted **shall** be maintained and archived.
- 2208 c. If during testing, the IUT version or subversion (e.g. pre-release, debug) changes, the
- 2209 final test report being submitted **shall** reflect the final version of the IUT.
- 2210 d. If there are multiple simultaneous testing activities occurring at the vendor site, a
- 2211 system of separation between the different cryptographic module test activities **shall** be
- 2212 maintained.
- 2213 e. For all conformance testing and validations, the CSTL **shall** ensure that any file
- 2214 containing iterative, not final, test results are isolated from the final test results.
- 2215 f. It is the CSTL's responsibility to ensure that any version iteration during the testing
- 2216 doesn't impact any of the final results transmitted to the CMVP.
- 2217 5. The required operational environment information (e.g., operating system name and
- 2218 version, processor family, hardware platform model) **shall** be obtained and verified
- 2219 against the operational environment information listed on the CAVP algorithm certificates
- 2220 for this module.
- 2221 6. The tester is accountable and therefore **shall** understand, oversee, direct, and/or assume
- 2222 control of testing operations to initialize, install, and operate the module. The tester is
- 2223 accountable to ensure the proper initialization, installation and operation of the module
- 2224 through the entire testing at the CSTL site and/or vendor site for the multiple testing
- 2225 sessions as applicable.
- 2226 7. If a test harness is used, it **shall** be reviewed or written by the lab. It **shall** be verified to
- 2227 have been maintained properly with no vendor manipulation prior to its execution. The
- 2228 test results on the remote operational environment **shall** be captured and transmitted back

2229 to lab without the risk of being modified. The tester **shall** verify the test harness runs
 2230 properly on its operational environment. The tester must verify the integrity of the testing
 2231 session as well as the completeness and accuracy of the test results.

2232 8. The remote testing **shall** cover the same set of FIPS 140-3 requirements including but not
 2233 limited to the following list, as if the operational environment were local to the tester:

2234 a. The services listed in the module Security Policy can be invoked or directed/overseen
 2235 and verified by the tester.

2236 b. For a module to be validated at Level 2 or 3 for ISO/IEC 19790:2012 Section 7.4.4,
 2237 the role-based or identity-based authentication **shall** be performed or
 2238 directed/overseen and verified by the tester.

2239 c. The failure of self-tests and the subsequent transition to an error state where module
 2240 data output interfaces are inhibited can be observed and verified by the tester.

2241 d. As applicable per IG 9.3.A, entropy has been effectively analyzed and received an
 2242 ESV for all specific OEs and/or platforms prior to submission.

2243 The vendor must provide a signed affirmation letter to the lab describing the remote testing
 2244 process and access control mechanism that allows the lab to perform the test on the remote
 2245 operational environment and protects the integrity of the test results. The lab **shall** provide a
 2246 signed letter to the CMVP stating that the module had been tested remotely, affirming that the
 2247 vendor provided their affirmation letter, stating what TEs were tested remotely, and explaining
 2248 how the requirements were met during the remote testing.

2249 It is the CSTL's responsibility to ensure that the assurance level is maintained when remote
 2250 testing is being conducted.

2251 Additional Comments:

2252 1. It is the responsibility of the tester to determine if a module is eligible to be tested remotely. If
 2253 the tester cannot demonstrate a test requirement during remote testing, then the module **shall** not
 2254 be fully tested remotely. If the tester wishes to test a subset of test requirements remotely, the
 2255 remaining test requirements **shall** be tested onsite at the CSTL site or in person by the CVP tester
 2256 at the vendor site.

2257 2. The tester **shall** confirm that the operational environment exactly matches the agreed upon test
 2258 environment, including any virtual environments used. A Virtual Machine may not be used in
 2259 lieu of an OS, unless the VM has been agreed to be part of the test environment and will be listed
 2260 on the certificate.

2261 3. A record of the testing location, related documentation (e.g. equipment proof of calibration)
 2262 and CSTL tester(s) who conducted the testing **shall** be maintained. This is applicable for all
 2263 tests including physical security testing.

2264 4. The above vendor site remote testing requirements are also applicable to 3rd party remote site
 2265 in addition to existing the HB 150-17 and NVLAP General Criteria Checklist ISO_IEC 17025
 2266 requirements.

2267 5. Regardless of the location of the testing, it is the CSTL's responsibility to ensure that all HB
 2268 150-17 and NVLAP General Criteria Checklist ISO_IEC 17025 requirements are met (e.g.
 2269 NVLAP General Criteria Checklist ISO_IEC 17025: 6.4.2, 6.4.3, 6.4.6, 6.4.7, 6.4.8, 6.4.13,
 2270 7.1.4, B.2.2 & B.3 requirements).

2271 6. Regarding any ITAR related questions, please refer to <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.54>.
 2272

2273 7.5 Partial validations and non-applicable areas

2274 CMVP will not issue a validation certificate unless the cryptographic module meets at least the
 2275 Security Level 1 requirements for each area in Section 6 of ISO/IEC 24759:2017. Areas can be
 2276 designated as Not Applicable (N/A) if they meet the following criteria:

- 2277 • Section 6.5, Software/Firmware Security may be designated as N/A if the module is
 2278 hardware-only without firmware or software;
- 2279 • Section 6.6, Operational Environment may be designated as N/A if the operational
 2280 environment for the cryptographic module is a limited or non-modifiable operational
 2281 environment and Section 6.7, Physical Security is greater than Security Level 1
 2282 (AS06.04).
- 2283 • Section 6.7, Physical Security may be designated as N/A if the cryptographic module is a
 2284 software-only module and thus has no physical protection mechanisms;
- 2285 • Section 6.8, Non-invasive security is N/A as there are currently no requirements in SP
 2286 800-140F. Any claims for non-invasive will be identified under Section 6.12.
- 2287 • Section 6.12, Mitigation of Other Attacks is Applicable if the module has been purposely
 2288 designed, built, and publicly documented to mitigate one or more specific attacks.
 2289 Otherwise, this section may be designated as N/A.

2290 7.6 CMVP requirements for PIV validations

2291 PIV card applications can only be tested on a CMVP validated module, such as a smartcard. The
 2292 CMVP validated module then obtains NPIVP validation, by adding the PIV card application to
 2293 the module. The validated smartcard and the PIV card application is then re-validated as a
 2294 CMVP module.

2295 A PIV card application that is included as a component of a cryptographic module **shall** be
 2296 referenced on the module validation. The cryptographic module validation entry **shall** provide
 2297 reference to the PIV card application(s) validation certificate number. The cryptographic
 2298 module's versioning information **shall** include the complete versioning information of the
 2299 module including the PIV application(s). Each PIV application's name **shall** be clearly
 2300 identified, and the PIV Certificate number is referenced on the CMVP module validation.

2301 The PIV NPIVP validation entry includes the following information:

- 2302 1. the name of the PIV card application,

- 2303 2. the name of the cryptographic module the PIV application was tested on, and
 2304 3. the complete versioning information of the module including the PIV application(s)

2305 The NPIVP validation entries can be found at:

2306 http://csrc.nist.gov/groups/SNS/piv/npivp/validation_lists/PIVCardApplicationValidationList.htm
 2307 [m](http://csrc.nist.gov/groups/SNS/piv/npivp/validation_lists/PIVCardApplicationValidationList.htm)

2308 7.7 Module count definition

2309 Moved to the following CMVP webpage, under “MIS Field Descriptions”:

2310 <https://csrc.nist.gov/projects/cmvp/sp800-140b>

2311 7.8 Module definitions for same certificates

2312 To be on the same certificate, each module version **shall** have identical:

- 2313 1. Section and overall levels.
 2314 2. Suite of approved security services.
 2315 3. Cryptography.
 2316 4. Suite of security functions and underlying algorithms, modes, and key sizes.
 2317 5. Suite of SSPs associated with the security services.
 2318 6. Suite of roles and authentication methods.
 2319 7. Finite State Model except related to the allowed differences.
 2320 8. SSP establishment methods.
 2321 9. Design assurance.
 2322 10. Mitigation of other attacks.
 2323 11. Module type (i.e., Software, Hardware, Firmware, or Hybrid).
 2324 12. Module embodiments (i.e., single-chip, multi-chip embedded/standalone) with similar
 2325 physical construction including physical boundary.

2326 7.9 Vendor or User Affirmation of Modules

2327 The tested/validated module version, OE upon which it was tested, and the originating vendor
 2328 are stated on the validation certificate entry. The certificate validation entry serves as the
 2329 benchmark for the module-compliant configuration. This guidance addresses two separate
 2330 scenarios: changes a **Vendor** (7.9.1) can affirm the module will perform as tested in the CSTL’s
 2331 validation submission and changes a **User** (7.9.2) can affirm the module will perform as tested in
 2332 the CSTL’s validation submission.

2333 This guidance is *not applicable* for validated modules when the requirements of **ISO/IEC**
 2334 **19790:2012** Section 7.7 Physical Security has been validated at Levels 2 or higher. This
 2335 guidance is however, applicable at Level 1 for *firmware* or *hybrid* modules.

2336 7.9.1 Vendor

2337 1. A vendor may perform post-validation recompilations of a software or firmware module and
 2338 affirm the modules continued validation compliance. By adding vendor support of non-tested
 2339 configurations to the validated module security policy, the vendor bears all responsibility.
 2340 These non-tested configurations versions may be considered by the user at their risk,
 2341 provided the following is maintained:

2342 a) Software modules that do not require any source code modifications (e.g., changes,
 2343 additions, or deletions of code) to be recompiled and ported to another OE must:

2344 i) For **Level 1 OE**, a software cryptographic module can be considered compliant with
 2345 the FIPS 140-3 validation when operating on any general-purpose platform/processor
 2346 that supports the specified operating system as listed on the validation entry or
 2347 another compatible⁴ operating system, or

2348 ii) For **Level 2 OE**, a software cryptographic module can be considered compliant with
 2349 the FIPS 140-3 validation when operating on any general-purpose platform/processor
 2350 that supports the same level 2 operational environment settings specified on the
 2351 validation entry.

2352 b) Firmware modules that do not require any source code modifications (e.g., changes,
 2353 additions, or deletions of code) to be recompiled, and its identified unchanged tested
 2354 operating system (i.e., same version or revision number) may be ported together from one
 2355 platform to another platform while maintaining the module's validation.

2356 Level 2 and above Firmware modules cannot be ported and maintain their validation,
 2357 since Physical Security must be retested.

2358 c) Hybrid modules may be ported together from one OE to another OE while maintaining
 2359 the module's validation provided that they do not require any of the following:

2360 i) software or firmware source code modifications (e.g., changes, additions, or deletions
 2361 of code) to be recompiled and its identified unchanged tested operating system (i.e.,
 2362 same version or revision number) or another compatible operating system;

2363 ii) modified hardware components utilized by the software or firmware (e.g., changes,
 2364 additions, or deletions).

2365 Level 2 and above hybrid modules cannot be ported and maintain their validation, since
 2366 Physical Security must be retested.

2367 The CMVP allows vendor porting and re-compilation of a validated software, firmware or
 2368 hybrid cryptographic module from the OE specified on the validation certificate to an OE
 2369 which was not included as part of the validation testing as long as the porting rules are
 2370 followed. Vendors may affirm that the module works correctly in the new OE. However, the
 2371 CMVP makes no statement as to the correct operation of the module or the security strengths

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.

2372 of the generated keys when so ported if the specific OE is not listed on the validation
2373 certificate.

2374 The vendor **shall** work with a CSTL to update the security policy and submit it to the CMVP
2375 under one of the available revalidation scenarios (see Scenario VAOE in Section 7.1). The
2376 update would affirm and include references to the new vendor affirmed OE(s) (see table in
2377 SP 800-140B and SP 800-140Brev1). The module's Security Policy **shall** include a statement
2378 that no claim can be made as to the correct operation of the module or the security strengths
2379 of the generated keys when ported to an OE which is not listed on the validation certificate.

2380 2. Software or firmware modules that require source code modifications (e.g., changes,
2381 additions, or deletions of code) to be recompiled and ported to another hardware or OE must
2382 be reviewed by a CSTL and revalidated per [Section 7.1](#) (including regression testing) to
2383 ensure that the module does not contain any OE-specific or hardware environment-specific
2384 code dependencies. See Scenarios UPDT, NSRL, and OEUP. This is not porting but rather
2385 incorporating the new versions and environment onto the certificate.
2386

2387 The vendor must meet all applicable requirements in ISO/IEC 19790:2012 Section 7.11, SP 800-
2388 140 Section 6.11, and CMVP IGs.

2389 7.9.2 User

2390 **A user may not modify a validated module. Any user modifications invalidate a module**
2391 **validation.**⁵

2392 A user may perform post-validation porting of a module and affirm the module's continued
2393 validation compliance provided the following is maintained:

2394 1. For **Level 1 OE**, a software, firmware, or hybrid cryptographic module will remain
2395 compliant with the FIPS 140-3 validation on any general-purpose platform/processor that
2396 supports the specified operating system listed on the validation entry, or another compatible
2397 operating system.

2398 The user may affirm that the module works correctly in the new OE if the porting rules are
2399 followed. However, the CMVP makes no statement as to the correct operation of the module or
2400 the security strengths of the generated keys when ported and executed in an OE not listed on the
2401 validation certificate.

2402 7.10 Operational Equivalency Testing for HW Modules

2403 CMVP requires full testing of any module that the vendor wishes to list on the certificate.
2404 However, modules may be grouped together if they are the same except for devices listed under
2405 Equivalence Categories, which are currently considered for five classes of devices. Each

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.

2406 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

2407 *Table 2 - Equivalence Categories*

2408 For details on the Equivalency Categories, please see the Equivalency Categories Tables under
 2409 the [FIPS 140-3 Resources Tab](#) of the CMVP website. Also note, for modules that have
 2410 differences within each of those categories, the level of testing required is dependent on the
 2411 differences. Some differences require analysis only, while others require full or limited
 2412 regression testing. The following are the general categories of the levels of testing. The actual
 2413 testing required depends on the Equivalency Category (See Equivalency Regression Test Table
 2414 and Equivalency Categories Tables found under the [FIPS 140-3 Resources Tab](#) of the CMVP
 2415 website):

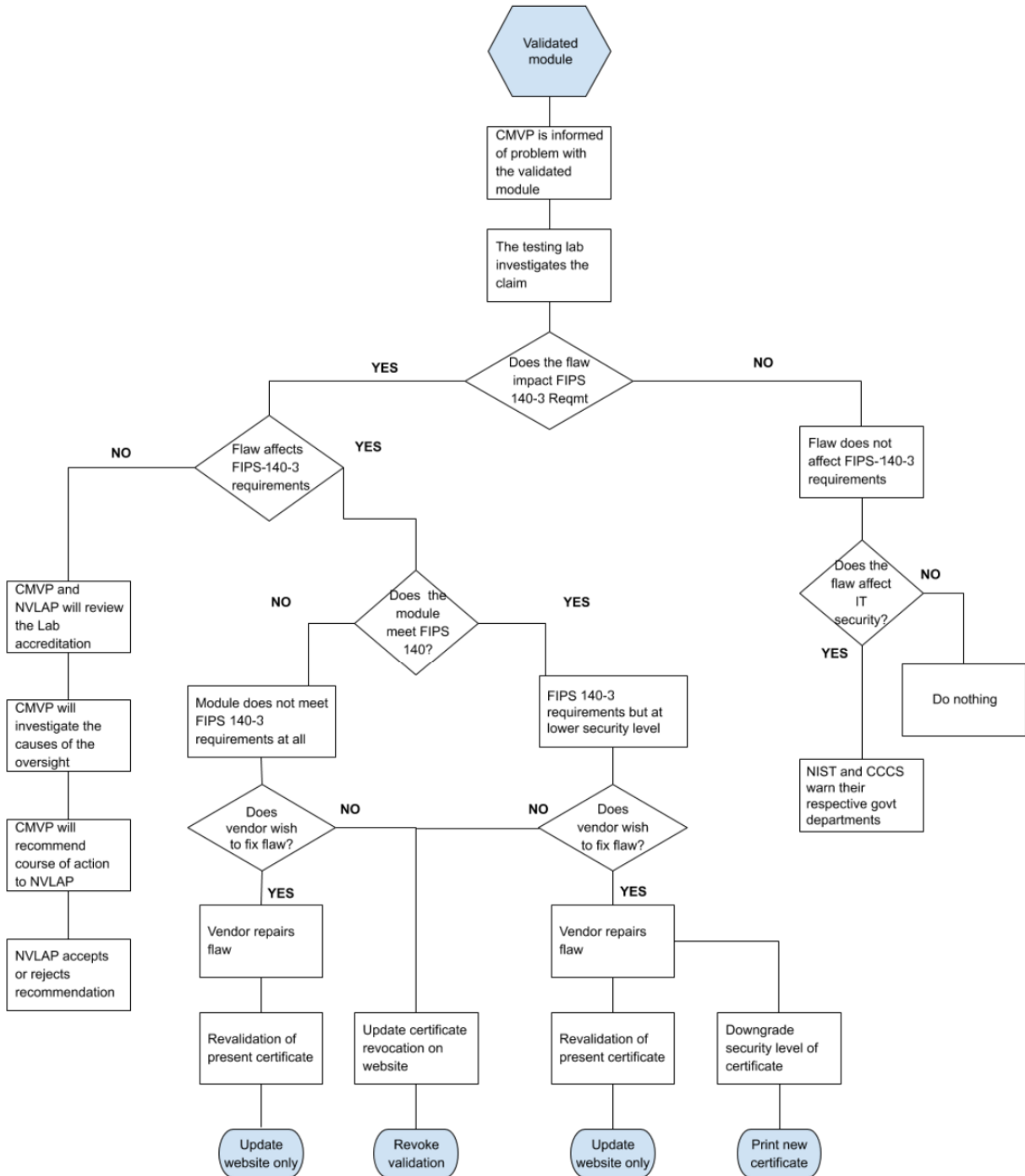
- 2416 - Analysis Only (AO) for Equivalency Category X: Once the equivalency evidence/argument
 2417 is provided and validated for the Equivalency Category X, there is no additional test other
 2418 than the proof of its physical existence required on a module with the equivalent components
 2419 in Category X to the module that has been fully tested under the same validation.
- 2420 - Required Testing (RT) for Equivalency Category X:
 - 2421 ○ If a module has some security relevant differences in the Equivalency Category X, the
 2422 module **shall** be tested against all of the listed TEs for that category in Equivalency
 2423 Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP website.
 - 2424 ○ If a module claims equivalency in multiple categories in comparison to a fully tested
 2425 module under the same validation, all of the required TEs for each claim equivalency
 2426 category **shall** be satisfied.

- 2427 - Focused Testing (FT) for Equivalency Category X:
- 2428 o The use of some technologies may introduce Security Relevant differences that cannot be
2429 predicted by this Section 7.10. For example, Programmable Logic Devices may be used
2430 to support the Cryptographic Module in a number of different ways that are security
2431 relevant (e.g., authentication). It is up to the lab to determine what section of the standard
2432 is affected by this security relevant difference and apply the Revalidation Regression Test
2433 Table found under the FIPS 140-3 Resources Tab of the CMVP website. For other
2434 sections not affected by this difference, Regression Testing per Equivalency Regression
2435 Test Table found under the FIPS 140-3 Resources Tab of the CMVP website shall be
2436 performed.
- 2437 - Complete Regression Testing (CRT): If an equivalency justification cannot be made, or the
2438 module differences can be mapped to a CRT entry within Equivalency Categories Tables
2439 under the FIPS 140-3 Resources Tab of the CMVP website, all modules, which lack an
2440 equivalency justification must, according to their security level, satisfy each TE listed in the
2441 Revalidation Regression Test Table under the FIPS 140-3 Resources Tab of the CMVP
2442 website.
- 2443 In each report where the vendor wishes to claim equivalency, the lab **shall**:
- 2444 - List the Equivalency Category, and specific component types being claimed in TE02.15.01.
2445 The lab must justify the component categorizations. The assumption is that the vendor
2446 initiated the Equivalency Category argument while the lab performed the analysis.
- 2447 - List the additional testing performed (if any) between the modules. This list **shall** be
2448 provided as an addendum to the test report.
- 2449 - Include in the Test Report how each module meets the TE's that are required for testing per
2450 this Section 7.10.
- 2451 For example:
- 2452 - Two devices to be on the same certificate have Hard Drives with different storage capacities,
2453 so testing requirement is Analysis Only, e.g., proof that both modules exist as claimed by the
2454 vendor.
- 2455 - Two devices to be on the same certificate have different types of Solid State Memory: one
2456 has NOR Flash and the other has NAND. This will require a small selection of testing, per
2457 Equivalency Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP
2458 website.
- 2459 - Two devices to be on the same certificate have different types of storage: one has a Hard
2460 Disk and the other has a Solid-State Drive. This will require complete regression testing per
2461 Revalidation Regression Test Table.
- 2462 Additional Comments
- 2463 - The lab shall perform full testing on at least one module.
- 2464 - This only applies to Operational testing of Hardware modules
- 2465 - Physical security testing (ISO/IEC 19790:2012, section 7.7) is not addressed for Security
2466 Level 2 and above. In other words, this does not exempt the lab from performing physical

- 2467 security testing for modules at Level 2 or above. This is because the lab needs to examine
2468 each module for, e.g., opacity and tamper evidence, if there are physical differences between
2469 the modules.
- 2470 - Components considered equivalent may still affect the entropy generated within the modules
2471 in different ways. This must be accounted for in the entropy report, if entropy is applicable.
 - 2472 - Equivalency considerations of the main processors/CPU's are out of scope of this Section
2473 7.10. If the CPU is different between modules on the same certificate, then the full
2474 Revalidation Regression Test Table must be run (found under the FIPS 140-3 Resources Tab
2475 of the CMVP website). If the entropy is OE based, the entropy must address the new OE.
 - 2476 - ISO/IEC 24759:2017 Section 6.7 Physical Security, Section 6.8 Non-Invasive Security and
2477 Section 6.12 Mitigation of Other Attacks are not applicable.
- 2478

2479 **Annex A CMVP Post Validation Issue Assessment Process**

2480 **Annex A.1 Addressing Security Relevant Issues**



2481
2482

Figure 5- Annex A. Validation Issue Assessment Process

2483 **Annex A.2 Addressing CVE Relevant Vulnerabilities**

2484 The list of CVEs is maintained by NIST in the NVD at <https://nvd.nist.gov/>. The purpose of the
2485 Scenario CVE revalidation (described in Section 7.1) is to provide the vendor a means to quickly
2486 fix, test and revalidate a module that is subject to a security-relevant CVE, while at the same
2487 time providing assurance that the module still meets the current FIPS 140 standards.

2488 Vendors **shall** reference this database and address the security relevant CVE's that are within the
2489 boundary of the module, not only during the validation process, but also after the module has
2490 been validated. Without published security relevant CVEs being addressed by the vendor and
2491 verified by the testing laboratory, the CMVP has no assurance that the module meets the
2492 requirements to obtain or maintain validation.

2493 At the discretion of the CMVP, certificates will be revoked that do not comply. It is the goal of
2494 the CMVP to maintain the security of validated modules.

2495 For more information about CVEs please also refer to <https://cve.mitre.org/>. See also [IG 11.A](#)
2496 [CVE Management](#) for more guidance on this topic.

ACRONYMS

2497

2498

2499	ANSI	American National Standards Institute
2500	AS	Assertion
2501	CAVP	Cryptographic Algorithm Validation Program
2502	CCCS	Canadian Centre for Cyber Security
2503	CMVP	Cryptographic Module Validation Program
2504	CSTL	Cryptographic and Security Testing Laboratory
2505	CVC	Consolidated Validation Certificate
2506	CVP	Cryptographic Validation Program
2507	DES	Data Encryption Standard
2508	ECR	Extended Cost Recovery
2509	ESV	Entropy Source Validation
2510	FIPS	Federal Information Processing Standard
2511	FISMA	Federal Information Security Management Act
2512	FSM	Finite State Model
2513	GC	Government of Canada
2514	HB	Handbook
2515	ID	Identification
2516	IG	Implementation Guidance
2517	ISO	International Organization for Standardization
2518	ITAR	International Traffic in Arms Regulation
2519	IUT	Implementation Under Test
2520	N/A	Not Applicable
2521	NCR	NIST Cost Recovery
2522	NECR	NIST Extended Cost Recovery
2523	NIST	National Institute of Standards and Technology
2524	NVLAP	National Voluntary Laboratory Accreditation Program
2525	OE	Operational Environment
2526	OS	Operating System
2527	PDF	Portable Document Format

2528	RFG	Request for Guidance
2529	SP	Special Publication
2530	TE	Tester Evidence
2531	TID	Tracking Identification Number
2532	TR	Test Requirements
2533	URL	Uniform Resource Locator
2534	VE	Vendor Evidence