

**FIPS 140-3**  
**Cryptographic Module Validation Program**  
**Management Manual**

**(Date 12/17/2024)**

**Version 2.3**

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

## Revision History

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

		<p>suspension.</p> <p>4.3.3 (<a href="#">Request for Transition Period Extension</a>): New section.</p> <p>6.2 (<a href="#">Suggested Tools for Physical Testing</a>): Added text in the first paragraph around calibration and a few other minor changes.</p> <p>7.1.1 (<a href="#">Requirements for all revalidations</a>): Updated guidance for new CSTLs.</p> <p>7.1.2.1 (<a href="#">Interim Validation</a>): New section.</p> <p>7.1.5 (<a href="#">Non-Security Relevant (NSRL)</a>): Added ‘d’ on minimum test requirements.</p> <p>7.8. (<a href="#">Module definitions for same certificates</a>): Added “self-tests”.</p>
--	--	--

# Table of Contents

## Contents

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	Background	1
1.2	Purpose of the CMVP Management Manual	1
1.3	Applicability and Scope	1
1.4	Purpose of the CMVP	1
1.5	Purpose of the Cryptographic Algorithm Validation Program (CAVP)	2
1.6	Use of Validated Products	2
1.7	CMVP Management Manual Structure	2
1.8	CMVP Related Documents	3
1.8.1	FIPS 140-3	3
1.8.2	Security Requirements for Cryptographic Modules	3
1.8.3	Test requirements for cryptographic modules	4
1.8.4	NIST SP 800-140x	4
1.8.5	Implementation Guidance	5
1.8.6	Web Cryptik User Guide	5
1.8.7	CSTL Accreditation Standards	6
1.8.8	Page Links on the CMVP Website Main Page	6
<b>2</b>	<b>CMVP MANAGEMENT</b>	<b>9</b>
2.1	Introduction	9
2.2	Validation Authority	9
2.3	Programmatic Directives, Policies, Internal Guidance and Documentation	9
2.4	CMVP Points of Contact	9
2.4.1	Language of Correspondence	10
2.5	Request for Guidance from CMVP	10
2.5.1	Request for Guidance Details	11
2.5.2	Request for Guidance Format	12
2.5.3	Post Validation Inquiries	12
2.6	Roles and Responsibilities of Program Participants	13
2.6.1	Vendor	13
2.6.2	Cryptographic and Security Testing Laboratory	13
2.6.3	CMVP Validation Authorities	15
2.6.4	Validated Module User	15

<b>2.7</b>	<b>CMVP Meetings</b>	<b>15</b>
2.7.1	CSTL Manager Meetings	16
2.7.2	CMUF participation	16
<b>2.8</b>	<b>Confidentiality of Information</b>	<b>16</b>
<b>3</b>	<b>CSTL PROCESSES</b>	<b>18</b>
<b>3.1</b>	<b>Accreditation of CMVP scopes for CSTLs</b>	<b>18</b>
3.1.1	Accreditation Process for the CMVP scope	18
<b>3.2</b>	<b>Maintenance of CSTL Accreditation</b>	<b>22</b>
3.2.1	Proficiency of CSTL	22
3.2.2	Renewal of Accreditation	23
3.2.3	Ownership of a CSTL	23
3.2.4	Relocation of a CSTL	23
3.2.5	Change of Approved Signatories	23
3.2.6	Change of Key Laboratory Testing Staff	24
3.2.7	Monitoring Visits	24
3.2.8	Extended Cost Recovery	24
3.2.9	Suspension of Accreditation	26
3.2.10	Revocation of Scope	26
<b>3.3</b>	<b>Confidentiality of Proprietary Information</b>	<b>26</b>
3.3.1	Confidentiality of Proprietary Information Exchanged between NIST, CCCS and the CSTL	26
3.3.2	Non-Disclosure Agreement for Current and Former Employees	27
<b>3.4</b>	<b>Code of Ethics for the CSTLs</b>	<b>27</b>
<b>3.5</b>	<b>Management of CMVP and CAVP Test Tools</b>	<b>27</b>
<b>4</b>	<b>CMVP PROCESSES</b>	<b>28</b>
<b>4.1</b>	<b>Cryptographic Module Validation Process Overview</b>	<b>28</b>
4.1.1	Vendor, CSTL, and CMVP duties for Testing of the Cryptographic Module	28
<b>4.2</b>	<b>Implementation Under Test (IUT) and Modules in Process (MIP)</b>	<b>31</b>
<b>4.3</b>	<b>Validation Submission Queue Processing</b>	<b>31</b>
4.3.1	Full and Update Submission Validations	31
4.3.2	All other submissions	31
4.3.3	Request for Transition Period Extension	32
4.3.4	HOLD Status for Cryptographic Modules on the Modules In Process	32
4.3.5	Resubmission while in Review Pending	33
4.3.6	Changes while in Coordination	33
4.3.7	Validation Deadline	34
<b>4.4</b>	<b>Validation when Test Reports are not Reviewed by both Validation Authorities</b>	<b>34</b>
4.4.1	Controlled Unclassified Information	34
<b>4.5</b>	<b>CMVP Fees</b>	<b>36</b>
4.5.1	Cost Recovery Program (CR & ECR)	36
4.5.2	NIST Payment Policy	36
4.5.3	Invoice for a Report Submission	36

<b>4.6</b>	<b>Flaw Discovery Handling Process</b>	<b>37</b>
<b>4.7</b>	<b>Historical or Revoked Validations</b>	<b>37</b>
<b>4.8</b>	<b>Entropy Source Validation (ESV) Processes</b>	<b>38</b>
4.8.1.1	Entropy Source Validation Submissions	39
4.8.1.2	Entropy Source Validation Web Client	40
4.8.1.3	Entropy Source Validation Python Client	40
4.8.2	Entropy Source Validation Comment Remediation Process	41
4.8.3	Entropy Source Validation Webpages	41
<b>4.9</b>	<b>CMVP Webpages</b>	<b>41</b>
4.9.1	Official CMVP Website	41
4.9.2	Cryptographic Module Validation Lists	41
4.9.3	CMVP Certificate Page Links	43
4.9.3.1	Security Policy	43
4.9.3.2	Consolidated Validation Certificate	43
4.9.3.3	Vendor Link	43
4.9.3.4	Vendor Product Link	43
4.9.3.5	Algorithm Certificates	43
4.9.3.6	Validation History	44
4.9.4	Usage of FIPS 140-3 Logos	44
<b>5</b>	<b>CMVP AND CAVP PROGRAMMATIC METRICS COLLECTION</b>	<b>45</b>
<b>5.1</b>	<b>Overview</b>	<b>45</b>
<b>5.2</b>	<b>Confidentiality of the Collected Metrics Data</b>	<b>45</b>
<b>5.3</b>	<b>Collected Metrics</b>	<b>45</b>
<b>6</b>	<b>TEST TOOLS</b>	<b>46</b>
<b>6.1</b>	<b>Web Cryptik</b>	<b>46</b>
<b>6.2</b>	<b>Suggested Tools for Physical Testing</b>	<b>46</b>
<b>7</b>	<b>CMVP GENERAL TESTING AND REPORTING GUIDANCE</b>	<b>48</b>
<b>7.1</b>	<b>Submission Scenarios</b>	<b>48</b>
7.1.1	Requirements for all revalidations	48
7.1.2	Full Submission (FS)	49
7.1.2.1	Interim Validation	50
7.1.3	Vendor Update (VUP)	50
7.1.4	Vendor Affirmed Operational Environment (VAOE)	50
7.1.5	Non-Security Relevant (NSRL)	50
7.1.6	Algorithm Update (ALG)	52
7.1.7	Operational Environment Update (OEUP)	52
7.1.8	Rebrand (RBND)	53
7.1.9	Port Sub Chip (PTSC)	54
7.1.10	Update (UPDT)	55
7.1.11	Common Vulnerabilities and Exposures (CVE)	56
7.1.12	Algorithm Transition (TRNS)	57
7.1.13	Physical Enclosure (PHYS)	61
7.1.14	Submission Scenario Summary Table	62

7.1.15	Additional Comments	63
<b>7.2</b>	<b>CMVP requirements pertaining to testing and approved algorithms</b>	<b>64</b>
7.2.1	Vendor Affirmation of Security Functions and Methods	65
7.2.2	Transitioning from vendor affirmed to CAVP Testing	65
<b>7.3</b>	<b>Testing using Emulators and Simulators</b>	<b>66</b>
<b>7.4</b>	<b>Remote Testing of Modules</b>	<b>68</b>
<b>7.5</b>	<b>Partial validations and non-applicable areas</b>	<b>71</b>
<b>7.6</b>	<b>CMVP requirements for PIV validations</b>	<b>71</b>
<b>7.7</b>	<b>Module count definition</b>	<b>72</b>
<b>7.8</b>	<b>Module definitions for same certificates</b>	<b>72</b>
<b>7.9</b>	<b>Vendor or User Affirmation of Modules</b>	<b>72</b>
7.9.1	Vendor	73
7.9.2	User	74
<b>7.10</b>	<b>Operational Equivalency Testing for HW Modules</b>	<b>74</b>
<b>ANNEX A</b>	<b>CMVP POST VALIDATION ISSUE ASSESSMENT PROCESS</b>	<b>78</b>
<b>Annex A.1</b>	<b>Addressing Security Relevant Issues</b>	<b>78</b>
<b>Annex A.2</b>	<b>Addressing CVE Relevant Vulnerabilities</b>	<b>79</b>

**ACRONYMS 80**

List of Figures

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

List of Tables

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

# 1 Introduction

## 2 1.1 Background

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

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

## 17 1.2 Purpose of the CMVP Management Manual

18 The purpose of the CMVP Management Manual is to provide effective guidance for managing  
19 the CMVP as authorized by FIPS 140-3 and conducting activities necessary to ensure that the  
20 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 that 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](http://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](http://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 800-140Br1** 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 800-140Cr2** replaces the approved security functions of ISO/IEC 19790:2012 Annex  
150 C. 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 800-140Dr2** 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/fips-140-3-ig-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements)  
173 [announcements](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements).

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

#### 175 1.8.6 Web Cryptik User Guide

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

185

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

## 187 1.8.7 CSTL Accreditation Standards

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

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

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

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

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

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

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

## 197 1.8.8 Page Links on the CMVP Website Main Page

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

199 1. Announcements ([https://csrc.nist.gov/Projects/Cryptographic-Module-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Announcements)  
200 [Validation-Program/Announcements](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Announcements)) contains information on changes made to  
201 documents or test tools.

202 2. Archived Notices ([https://csrc.nist.gov/Projects/Cryptographic-Module-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Notices)  
203 [Validation-Program/Notices](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Notices)) contains copies of statements published in the  
204 Federal Register, programmatic or policy updates or information not related to  
205 CMVP documents or test tools.

206 3. Validated Modules ([https://csrc.nist.gov/Projects/Cryptographic-Module-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules)  
207 [Validation-Program/Validated-Modules](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules)) contains a link to the search tool for finding  
208 a specific module or aspects of module validation. In addition, the page contains  
209 information describing categories (active, historical, and revoked) and explains the  
210 difference between a module that is a product and one that is a component.

211 4. Implementation Under Test (IUT) List  
212 ([https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List)  
213 [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  
214 cryptographic modules undergoing testing. The result of the testing has not yet been  
215 submitted to the CMVP. Inclusion of a module on this list is voluntary, dependent on  
216 the vendor. The CMVP has no information regarding the status of these modules and  
217 does not know if or when a test report will be submitted to the CMVP. The modules  
218 are listed by vendor name. For more information regarding a specific module, please  
219 contact the vendor.

220 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)  
221 [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  
222 review status for each cryptographic module whose scenario type is FS (Full  
223 submission) or UPDT (Update). The list tracks the test report after it has been  
224 submitted to the CMVP through validation. For each submission, the status and the  
225 date it went into that state is listed. The date will also be updated for any new

- 226 submission to the CMVP, even if the status remains the same. For additional  
227 information regarding a specific module, please contact the vendor.
- 228 6. Entropy Validations
- 229 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-  
231 validations](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-<br/>230 validations)) This has a search page, announcements, and documents pertaining to the  
Entropy Validations.
- 232 7. Programmatic Transitions ([https://csrc.nist.gov/Projects/cryptographic-module-  
234 validation-program/programmatic-transitions](https://csrc.nist.gov/Projects/cryptographic-module-<br/>233 validation-program/programmatic-transitions)) lists algorithm-related transitions.  
Applicable standards, relevant IGs, ACVTS availability, and the beginning CMVP  
235 acceptance date are listed for each algorithm/scheme. Also available is information  
236 related to deprecated algorithms/schemes that force validated module certificates to  
237 the historical category. Included in this list are deadlines for last submission date as  
238 an approved algorithm/scheme as well as the date whereby the validation certificate  
239 of an approved module using the algorithm/scheme will be moved to the Historical  
240 list.
- 241 8. CMVP FIPS 140-3 Management Manual  
242 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-  
244 140-3-management-manual](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-<br/>243 140-3-management-manual)) contains the link to the latest version of this manual.
- 244 9. CMVP FIPS 140-3 Related References  
245 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-  
247 standards](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-<br/>246 standards)) describes the FIPS 140-3 standard, referenced standards in FIPS 140-3,  
and CMVP management documents.
- 248 10. FIPS 140-3 IG Announcements ([https://csrc.nist.gov/Projects/cryptographic-  
250 module-validation-program/fips-140-3-ig-announcements](https://csrc.nist.gov/Projects/cryptographic-<br/>249 module-validation-program/fips-140-3-ig-announcements)) is where the latest version  
251 of the FIPS 140-3 IGs can be found. The webpage also includes a short summary of  
changes.
- 252 11. FIPS 140-3 Resources ([https://csrc.nist.gov/Projects/cryptographic-module-  
254 validation-program/140-3-resources](https://csrc.nist.gov/Projects/cryptographic-module-<br/>253 validation-program/140-3-resources)) provides guidance that is easily bookmarked.  
Information that is needed by vendors and CSTLs is listed here. As an example,  
255 specifically detailed validation and re-validation information such as minimum testing  
256 requirements for revalidation and equivalency can be found here. TE Documentation  
257 Guidance is also available.
- 258 12. Use of FIPS 140-3 or FIPS 140-2 Logo and Phrases  
259 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/use-of-fips-  
261 140-2-logo-and-phrases](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/use-of-fips-<br/>260 140-2-logo-and-phrases)) References and information as to the proper use and  
registration of CMVP FIPS 140 validation logos.
- 262 13. SP 800-140 Series Supplemental Information  
263 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-  
265 series-supplemental-information](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-<br/>264 series-supplemental-information)) contains a table summarizing the SP 800-140x series  
266 publications and their relationships to ISO/IEC 19790:2012(E) and ISO/IEC  
24759:2017(E). The sub-pages of this webpage provide the supplemental information

267 associated with that SP 800-140x document.

268 14. CVP Certification Exam Information  
269 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-information)  
270 [certification-exam-information](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cvp-certification-exam-information)) In order to be a certified tester for a CSTL, an  
271 individual must pass this exam.

272 15. NIST Cost Recovery Fees  
273 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)  
274 [recovery-fees](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)) NIST fees paid by CSTL for validations depending on scenario.

275 16. CSTL Accreditation and Fees ([https://csrc.nist.gov/Projects/Testing-](https://csrc.nist.gov/Projects/Testing-Laboratories)  
276 [Laboratories](https://csrc.nist.gov/Projects/Testing-Laboratories)) contains a link to the name and location of every CSTL accredited to  
277 perform Cryptographic and Security Testing. The list also includes a point of contact  
278 for each CSTL.

279 17. CMVP Validation Process  
280 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)  
281 [recovery-fees](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees)) Process flow showing the interactions between the CSTL, the Vendor,  
282 and the CMVP throughout the validation process.

283

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

285 **2 CMVP Management**

286 **2.1 Introduction**

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

289 **2.2 Validation Authority**

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

294 **2.3 Programmatic Directives, Policies, Internal Guidance and Documentation**

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

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

302 **2.4 CMVP Points of Contact**

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

306 The email address [cmvp@nist.gov](mailto:cmvp@nist.gov) will be used for the general public to contact NIST CMVP  
 307 and will continue to be published on the website as the main CMVP email account for NIST. The  
 308 [cmvp@cyber.gc.ca](mailto:cmvp@cyber.gc.ca) email address will continue to be separately supported and used by the CCCS  
 309 CMVP office.

310

311 Please direct all CMVP communication to both email addresses as shown below.

General Information Email Address	Purpose and Use
<a href="mailto:cmvp@cyber.gc.ca">cmvp@cyber.gc.ca</a>	All correspondence and FIPS 140-2 submissions to the CCCS CMVP.
<a href="mailto:cmvp@nist.gov">cmvp@nist.gov</a>	General correspondence to the NIST CMVP.

<a href="mailto:sp800-140-comments@nist.gov">sp800-140-comments@nist.gov</a>	Comments on CMVP guidance using the CMVP comment template.
--	--

312

313 The NIST CMVP uses some additional emails for specific CSTL communications. For more  
 314 information see the table below. Please only use the single email address required. PGP is used  
 315 for encrypted email.

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

316

317 Note1: In general, if you have been in direct email communication with a CMVP member then  
 318 continue to email them.

319 Note 2: General CSTL correspondence to [cmvplab@nist.gov](mailto:cmvplab@nist.gov) should also be sent to  
 320 [cmvp@cyber.gc.ca](mailto:cmvp@cyber.gc.ca) unless the matter only relates to NIST.

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

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

327 **2.4.1 Language of Correspondence**

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

330 **2.5 Request for Guidance from CMVP**

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

333 may be readily available. The information found on the CMVP website provides the official  
334 position of the CMVP. If the information cannot be found in the aforementioned guidance,  
335 CMVP will accept requests that are general knowledge or to a specific application. In addition,  
336 CMVP will accept post-validation inquiries for any perceived issues relating to existing modules.

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

340 Once a vendor is under contract with a CSTL, NIST/CCCS will only provide official guidance  
341 and clarification for the vendor's module through the point of contact at the CSTL. In a situation  
342 where the vendor and CSTL are at an irresolvable impasse over a testing issue, the vendor may  
343 ask for clarification/resolution directly from NIST/CCCS. The point of contact at the CSTL must  
344 be included in the distribution of this correspondence. All correspondence from NIST/CCCS to  
345 the vendor on the issue will be issued through the CSTL point of contact. If a vendor has an RFG  
346 inquiry that is not associated with a module submission through a CSTL, direct your  
347 communications to both [cmvp@nist.gov](mailto:cmvp@nist.gov) and [cmvp@cyber.gc.ca](mailto:cmvp@cyber.gc.ca). Do not send the requests to  
348 individuals.

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

354 **CSTLs** must submit all test-specific questions in the Request for Guidance (RFG) format  
355 described below. These questions must be submitted to [cmvplab@nist.gov](mailto:cmvplab@nist.gov) and  
356 [cmvp@cyber.gc.ca](mailto:cmvp@cyber.gc.ca).

### 357 2.5.1 Request for Guidance Details

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

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

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

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

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

372 Example 2: [99-FIPS140-3-RFG-CSTL\\_A-230630-1](#)

373 Example 3: [99-FIPS140-3-RFG-CSTL\\_A-230630-2](#)

374

375 If an International Traffic in Arms Regulations (ITAR) RFG submission, email

376 [cmvpitar@nist.gov](mailto:cmvpitar@nist.gov) **only** using PGP encryption, and indicate it is “ITAR” appended to “RFG”.

377 E.g.: 99-FIPS140-3-RFG\_ITAR-CSTL\_A-230630-1.

## 378 2.5.2 Request for Guidance Format

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

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

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

## 382 2.5.3 Post Validation Inquiries

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

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

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

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

401 1. is without merit and the validation of the module is unchanged.

402 2. has merit and the validation of the module is affected. The CSTL will further state its  
403 recommendations regarding the impact to the validation.

404 The CMVP will review the CSTL’s position and rationale supporting its conclusion. If the  
405 CMVP concurs that the official request is without merit, no further action is taken. If the CMVP  
406 concurs that the official request has merit, a security risk assessment will be performed regarding  
407 the non-conformance issue. Please see 1.1.1.1 Annex A for the flow diagram illustrating the  
408 assessment process.

409 **2.6 Roles and Responsibilities of Program Participants**

410 The various roles and responsibilities of the participants in the CMVP are illustrated in Figure 1  
 411 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

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

413 **2.6.1 Vendor**

414 The role of the vendor is to design and produce cryptographic modules that comply with the  
 415 requirements specified in the applicable ISO/IEC standards and NIST SPs. Among other  
 416 functions, the vendor defines the boundary of the cryptographic module, determines its modes of  
 417 operation and its associated services, and develops an entropy and algorithm strategy and provide  
 418 the information for the non-proprietary security policy. The security policy generation  
 419 information can be found in [https://csrc.nist.gov/Projects/cryptographic-module-validation-  
 420 program/sp-800-140-series-supplemental-information/sp800-140b](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-series-supplemental-information/sp800-140b). When a cryptographic  
 421 module is ready for testing, the vendor submits the module and the associated documentation to  
 422 the accredited CSTL of its choice.

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

426 **2.6.2 Cryptographic and Security Testing Laboratory**

427 The role of the CSTL is to independently test the cryptographic module to the requirements  
 428 defined for the FIPS 140-3 security level and embodiment, and to produce a written test report  
 429 for the CMVP Validation Authorities based on its findings. The CSTL can conduct algorithmic  
 430 testing and verify compliance with the algorithm standards (there may be additional requirements  
 431 beyond what is CAVP-tested), review the cryptographic module’s documentation and source  
 432 code, and perform the required testing of the module in accordance with the TR, SP 800-140x  
 433 and IG. All testing is performed or witnessed by a CVP tester. If a cryptographic module  
 434 conforms to all the requirements of the standards, the CSTL submits a written report to the  
 435 Validation Authority (CMVP). If a cryptographic module does not meet one (or more)  
 436 requirements, the CSTL may work with the vendor to resolve all discrepancies prior to  
 437 submitting the validation package to the Validation Authority. The CSTL reports to the vendor  
 438 any implementations do not meet the FIPS 140-3 testing requirements. CSTLs can not submit  
 439 non-conformant modules to the CMVP for validation without penalties.

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

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

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

### 478 2.6.3 CMVP Validation Authorities

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

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

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

### 495 2.6.4 Validated Module User

496 The user verifies that a cryptographic module that they are considering procuring has been  
497 validated and meets their requirements. A listing of validated cryptographic modules is  
498 available from [https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-  
499 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  
500 each validated cryptographic module so that a potential user can determine if the validated  
501 cryptographic module provides cryptographic services and protection required for their  
502 particular application and threat environment.

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

506 Users can also develop product or system specifications that include the requirements for FIPS  
507 140-3 validated cryptographic modules. It is important to note that a cryptographic module may  
508 be a complete product or a component thereof. Therefore, understanding the boundary and  
509 interface of the validated cryptographic module will help in the determination of an adequate  
510 cryptographic product.

## 511 2.7 CMVP Meetings

512 The CMVP is jointly managed by NIST and CCCS. Decisions are made jointly by both  
513 organizations, and the NIST and CCCS Program Managers communicate regularly. While most  
514 CMVP internal meetings focus on interactions with the CSTL, the CSTL Manager Meeting is  
515 focused on assessments and improvements of the CMVP program operations and management.

### 516 2.7.1 CSTL Manager Meetings

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

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

- 525 ● Status of the CMVP
- 526 ● Changed or new CMVP processes and/or procedures
- 527 ● Standards updates
- 528 ● Laboratory accreditation process update news
- 529 ● Implementation Guidance in development
- 530 ● Status of the CAVP
- 531 ● Test tool development
- 532 ● Upcoming meetings and/or symposiums

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

### 536 2.7.2 CMUF participation

537 The Cryptographic Module User Forum (CMUF) ([cmuf.org](http://cmuf.org)) was established in 2013 by module  
538 vendors, users, and CSTLs to provide a platform for practitioners in the community of  
539 UNCLASSIFIED Cryptographic Module (CM) and UNCLASSIFIED Cryptographic Algorithm  
540 (CA) Validation Programs (VP). The CMUF formed the annual ICMC which was held along  
541 with the CSTL manager meetings. CMVP participated in the Conference and found the ICMC to  
542 be an excellent way to communicate with the community at large.

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

## 550 2.8 Confidentiality of Information

551 The protection of vendor proprietary information is paramount to the success and credibility of

552 the CMVP and CAVP. Proper safeguards must be implemented by NIST, CCCS, and the CSTLs  
553 to protect against unauthorized disclosure of vendors' proprietary information. Any potential or  
554 actual breach of confidentiality could have an adverse effect on the NIST, CCCS, a CSTL's  
555 accreditation, or the program.

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

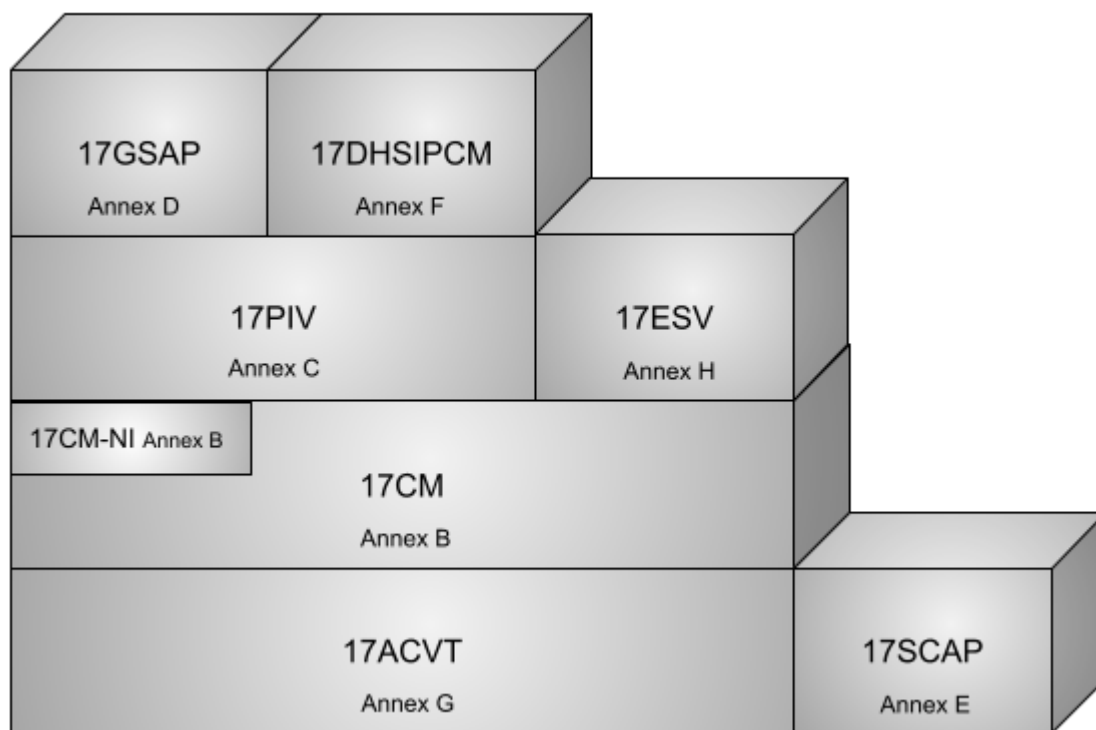
561 NIST, CCCS, and the CSTLs must ensure that personnel joining or departing these organizations  
562 are advised of their responsibilities about safeguarding the vendor proprietary information they  
563 may have been authorized to access during their period of employment.

564 **3 CSTL Processes**

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

568 **3.1 Accreditation of CMVP scopes for CSTLs**

569 This section describes in general terms the process for a laboratory to become an accredited  
 570 CSTL for scope 17CM under the National Voluntary Laboratory Accreditation Program  
 571 (NVLAP). Candidate laboratories may optionally apply for NVLAP 17CM-NI at the same time.  
 572 17ESV is also supported by CMVP, though is considered a separate program. Laboratories are  
 573 responsible for complying with the Cryptographic and Security Testing LAP which can be found  
 574 at <https://www.nist.gov/nvlap/cryptographic-and-security-testing-lap>.



575  
 576 *Figure 2 - CSTL NVLAP scopes*

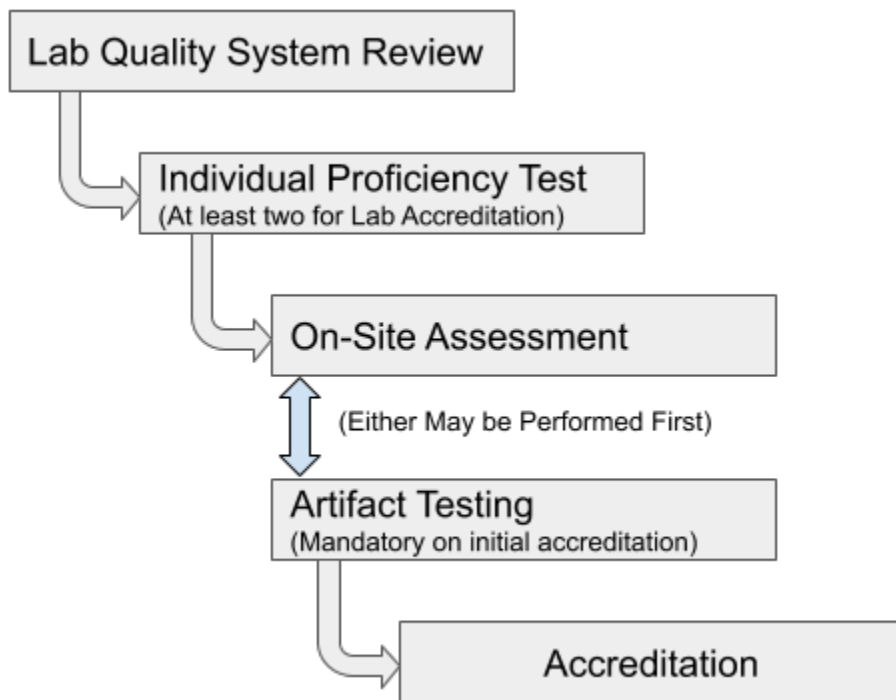
577 **NOTE:** Accreditation of the CAVP scope is necessary to obtain the 17CM scope for CMVP  
 578 testing laboratories. For more information about CAVP accreditation, please see **Becoming a**  
 579 **17ACVT Laboratory** on the CAVP website [https://csrc.nist.gov/Projects/cryptographic-](https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/how-to-access-acvts)  
 580 [algorithm-validation-program/how-to-access-acvts](https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/how-to-access-acvts).

581 3.1.1 Accreditation Process for the CMVP scope

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

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

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



589  
 590 *Figure 3 - CSTL Accreditation Process*

591 3.1.1.1 Application for Accreditation and Selection of Assessment Team

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

600 3.1.1.2 Management System Evaluation

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

603 3.1.1.3 CVP Proficiency Examination

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

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

- 610 • Physical Security
  - 611 ○ Understand the different module types and different embodiments for
  - 612 modules.
  - 613 ○ Understand requirements for physical security for modules specific to levels 1-
  - 614 4.
- 615 • Authentication, Roles, Services, Software/Firmware Security and Operational  
616 Environment
  - 617 ○ Understand authentication requirements and concepts.
  - 618 ○ Define the requirements for roles.
  - 619 ○ Understand the concepts of services using approved and non-approved
  - 620 functions, and the bypass capability.
  - 621 ○ Understand the self-initiated cryptographic output capability,
  - 622 Software/Firmware security including loading requirements and their
  - 623 applicability.
  - 624 ○ Describe the operational environment requirements/concepts and how to test
  - 625 them.
- 626 • Algorithms and Self-Tests
  - 627 ○ Understand the concepts of the approved and allowed algorithms.
  - 628 ○ Identify which algorithms are approved or allowed.
  - 629 ○ Identify testing for components of the algorithms.
  - 630 ○ Identify the tester's responsibilities when reviewing an algorithm's
  - 631 implementation.
  - 632 ○ Identify the pre-operational self-tests (e.g., integrity, bypass) and know the
  - 633 associated requirements.
  - 634 ○ Understand the requirements for conditional self-tests, including cryptographic
  - 635 algorithm self-tests.
- 636 • Sensitive Security Parameter (SSP) Establishment
  - 637 ○ Understand the requirements for SSP generation, SSP agreement, SSP
  - 638 transport and SSP derivation and applicable standards and guidance.
  - 639 ○ Understand and identify the approved random bit generators.
  - 640 ○ Understand the notion of entropy and methods of entropy estimation.
  - 641 ○ Possess general knowledge of the SSP establishment protocols and standards
  - 642 in the IT industry.

- 643 • SSP Management
  - 644 ○ Understand the requirements for SSP entry and output and trusted channels.
  - 645 ○ Understand the requirements for SSP storage.
  - 646 ○ Understand the various types of SSPs and their zeroization requirements.
- 647 • Security Assurances
  - 648 ○ Understand the requirements of module specification including degraded
  - 649 operation, approved and non-approved modes.
  - 650 ○ Understand the programmatic guidance and associated documentation
  - 651 requirements.
  - 652 ○ Understand the requirements for ports & interfaces, finite state model,
  - 653 development, mitigation of non-invasive and other attacks, and design
  - 654 assurance.

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

#### 665 3.1.1.4 On-Site Assessment

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

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

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

#### 677 3.1.1.5 Artifact Testing

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

### 683 3.1.1.6 Accreditation Decision

684 The CMVP will make a recommendation of the applicant laboratory competency. NVLAP will  
685 evaluate the results of the laboratory assessment and the CMVP recommendation, before making  
686 the final accreditation decision.

### 687 3.1.1.7 Granting Accreditation

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

- 690 • January 1
- 691 • April 1
- 692 • July 1
- 693 • October 1

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

### 699 3.1.1.8 CMVP Test Tools

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

### 708 3.1.1.9 Cooperative Research and Development Agreement

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

## 717 **3.2 Maintenance of CSTL Accreditation**

### 718 3.2.1 Proficiency of CSTL

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

722 the validation authority to demonstrate continued testing proficiency.

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

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

### 728 3.2.2 Renewal of Accreditation

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

734 The re-accreditation process is the same as illustrated in Figure 3 - CSTL Accreditation Process  
735 and described in Section 3.1.1 above. If deficiencies are found during the assessment of an  
736 accredited CSTL, the laboratory must submit to NVLAP a satisfactory plan outlining the  
737 resolution of deficiencies within thirty days of notification. On-site assessments of accredited  
738 laboratories are performed in accordance with the procedures in Section 3.3 of NIST Handbook  
739 150.

### 740 3.2.3 Ownership of a CSTL

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

### 745 3.2.4 Relocation of a CSTL

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

### 754 3.2.5 Change of Approved Signatories

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

759 3.2.6 Change of Key Laboratory Testing Staff

760 Key personnel include:

- 761 a. laboratory director;
- 762 b. laboratory manager(s);
- 763 c. staff members(s) responsible for maintaining management system;
- 764 d. authorized representative;
- 765 e. approved signatories; and
- 766 f. other key technical persons in the laboratory (e.g., testers).

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

772 3.2.7 Monitoring Visits

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

778 3.2.8 Extended Cost Recovery

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

781

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

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

782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792

General ECR guidance:

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

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

797  
798 If a CSTL has reached 6 or more points through the ECR process, the CMVP recommends the  
799 following actions to pre-empt suspension:

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

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

### 807 3.2.9 Suspension of Accreditation

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

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

- 815 1. reports submitted for validation within the accreditation cycle are incorrect, invalid, or  
816 deficient as defined by each validation program (see 3.2.8);
- 817 2. the loss of key technical personnel from the CSTL;
- 818 3. nonconformities found during any onsite visit are not appropriately addressed through  
819 corrective actions taken by the CSTL; or
- 820 4. the CSTL has not submitted the required number of vendor product test reports to the  
821 validation authority within the accreditation cycle.

### 822 3.2.10 Revocation of Scope

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

## 833 3.3 Confidentiality of Proprietary Information

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

### 836 3.3.1 Confidentiality of Proprietary Information Exchanged between NIST, CCCS and the CSTL

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

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

### 840 3.3.2 Non-Disclosure Agreement for Current and Former Employees

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

### 843 3.4 Code of Ethics for the CSTLs

844 The CSTL must:

- 845 1) Maintain NVLAP accreditation for the Cryptographic Security Testing Program;
- 846 2) Refrain from misrepresenting the scope of its accreditation;
- 847 3) Act legally and honestly;
- 848 4) Act ethically.

### 849 3.5 Management of CMVP and CAVP Test Tools

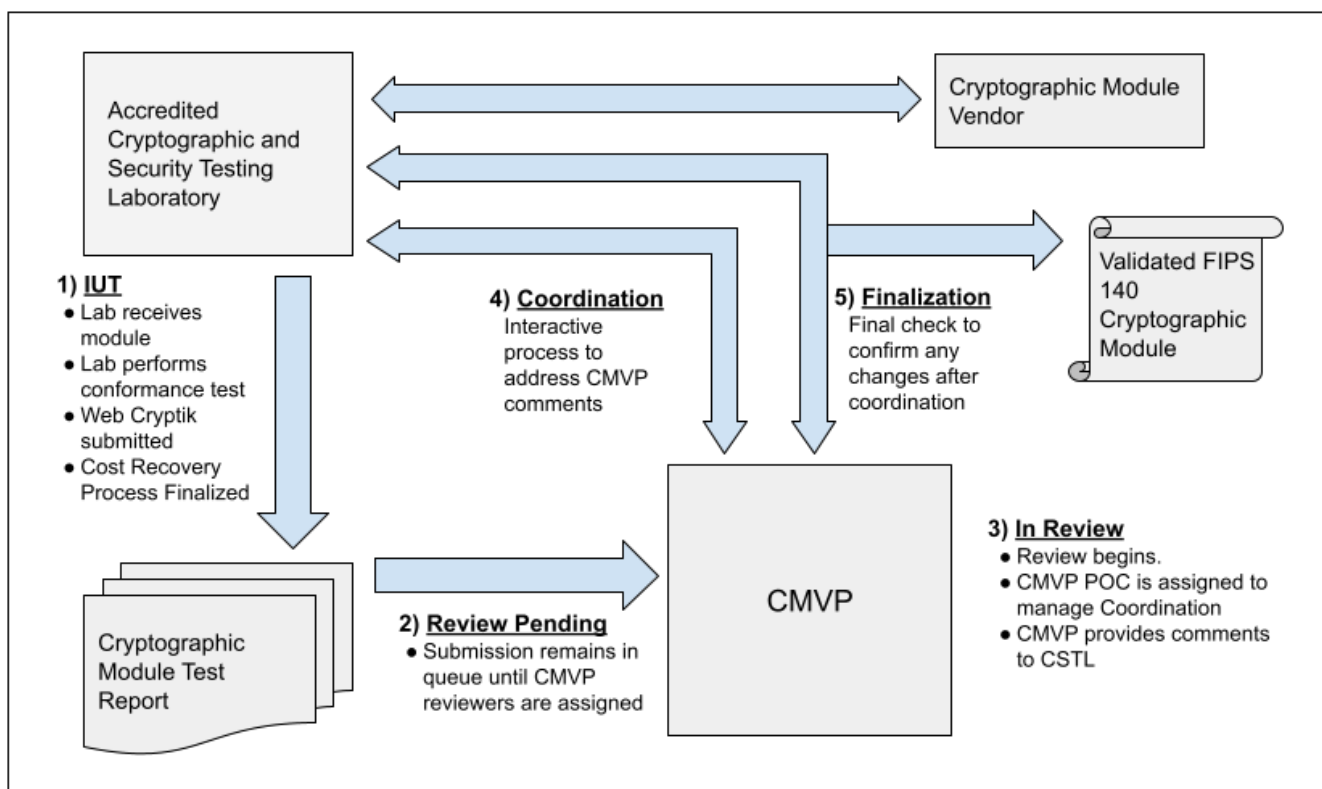
850 Test tools provided by NIST and CCCS must not be distributed to any entity outside the CSTL,  
851 including firms contracted by the CSTL, unless explicitly authorized by CMVP management.  
852 Personnel temporarily employed by and working under the supervision of a CSTL (i.e., a  
853 contractor)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

858 **4 CMVP Processes**

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

861 **4.1 Cryptographic Module Validation Process Overview**

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



867  
 868 *Figure 4- Cryptographic Module Testing and Validation Process*

869 **4.1.1 Vendor, CSTL, and CMVP duties for Testing of the Cryptographic Module**

870 A vendor contracts with an accredited CSTL to perform the cryptographic module validation  
 871 testing. The vendor provides the CSTL with the necessary documentation and either provides the  
 872 cryptographic module to the laboratory for testing or prepares it for testing at the vendor's  
 873 facility.

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

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

#### 879 4.1.1.1 Implementation Under Test

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

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

893 The cryptographic module validation process is an iterative process. At any point in the testing  
894 the CSTL may wish to request guidance from CCCS and NIST in determining how to apply the  
895 FIPS 140 standard to the particular cryptographic module. If the CSTL discovers any non-  
896 conformances in the cryptographic module documentation or the cryptographic module itself, it  
897 must bring details of the non-conformance(s) to the attention of the cryptographic module  
898 vendor. The cryptographic module vendor must correct the non-conformance(s) and resubmit  
899 updated documentation and the updated cryptographic module as necessary for validation  
900 testing.

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

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

#### 908 4.1.1.2 Review pending

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

914 At the CMVP's discretion, a test report in this state may be subject to a triaged review to quickly  
915 assess the quality of a report, and if needed, provide feedback to the lab. This triage activity is  
916 implemented based on common issues observed from the submissions received by the CMVP.  
917 Ability to quickly identify and address problematic submissions is paramount to not only  
918 advance the FIPS 140-3 queue, but also be fair to all labs and vendors. Problematic submissions

919 will be sent back to the labs accompanied by generic statements for resolution. These reports *will*  
920 maintain their respective queue positions.

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

#### 924 4.1.1.3 In Review

925 After the CMVP reviewers have been assigned to the submission, and the reviewer begins the  
926 review, the cryptographic module is moved to the IN REVIEW stage of the MIP List. The  
927 module validation must be completed and cannot exceed 24 months after transitioning to IN  
928 REVIEW. Once they have completed their review of the validation submission and provided  
929 comments, a comment file is sent to the CSTL. This event moves the cryptographic module to  
930 the COORDINATION stage, described in Section 4.1.1.4.

#### 931 4.1.1.4 Coordination

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

#### 940 4.1.1.5 Finalization

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

#### 945 4.1.1.6 Validation Certificate

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

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

## 959 4.2 Implementation Under Test (IUT) and Modules in Process (MIP)

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

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

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

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

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

## 977 4.3 Validation Submission Queue Processing

### 978 4.3.1 Full and Update Submission Validations

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

984 In cases whereby submissions are related to or dependent on other submissions, e.g., bound or  
985 embedded modules, the CMVP must be notified for consideration prior to their submission.  
986 CSTLs should also include this information in the special instructions field in Web Cryptik. This  
987 will allow CMVP to manage resources in support of these larger efforts. In general, and for  
988 dependent or related modules, testing must be completed prior to submission (including FIPS  
989 140-3 compliance testing and CAVP/ESV validations). In addition, prior to completion, the  
990 CSTL must review and address all changes from the completed validation.

### 991 4.3.2 All other submissions

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

### 994 4.3.3 Request for Transition Period Extension

995 Some Implementation Guidance is assigned a transition period before compliance to this  
 996 guidance is required; since meeting the guidance may likely require changes to cryptographic  
 997 modules or the functional testing of them as opposed to documentation changes. In some  
 998 instances, the transition period may not be long enough for the vendor to perform the  
 999 modifications needed to the cryptographic module for it to be compliant with the issued  
 1000 Implementation Guidance nor complete the additional cryptographic algorithm validation testing  
 1001 before the scheduled date for submission of the validation report.

1002 These situations will be reviewed on a case-by-case basis at the request of the CSTL performing  
 1003 the validation testing. A ruling will be made by the CMVP as to whether an extension can be  
 1004 granted for this particular requirement, for this particular cryptographic module, depending on  
 1005 the type of cryptographic module and the status of the validation testing.

### 1006 4.3.4 HOLD Status for Cryptographic Modules on the Modules In Process

1007 While a CSTL may request a HOLD, the status can be executed by the CMVP. There are several  
 1008 reasons that a submission review may be placed on HOLD status. Some of these reasons are as  
 1009 follows:

- 1010 1. If a module test report is sent incomplete or is determined to be incomplete once the  
 1011 module has moved to the IN REVIEW or a later stage-.
- 1012 2. When the ECR notification is sent to the CSTL, the module will be placed on HOLD. If  
 1013 the ECR has been paid and the CSTL resubmits the report, the HOLD is removed.
- 1014 3. If a non-compliance issue is discovered during the module review or coordination.
- 1015 4. If a module is dependent on the completion of another module (i.e., the case of  
 1016 bound/embedding), the dependent module may be placed on HOLD until the base  
 1017 validation has been completed. The CSTL must indicate the module dependency upon  
 1018 submission via Web Cryptik Special Instructions. If a submission is put on HOLD due  
 1019 to dependency, it is the responsibility of the CSTL to notify the CMVP when the initial  
 1020 submission is completed. This assures the CMVP will remove the hold for related or  
 1021 dependent submissions.
- 1022 5. During COORDINATION, CMVP comments are sent to the CSTL and if the CSTL has  
 1023 not responded within 90 calendar days, the module will be placed on HOLD. After 150  
 1024 calendar days, an email notification will be sent to indicate that if no submission is  
 1025 received in the next 30 calendar days (180 calendar days in total), the module will be  
 1026 dropped from the CMVP queue. The CSTL must inform the vendor of the CMVP's  
 1027 intent to drop the module due to the 6-month period of delay. If the CSTL cannot  
 1028 respond to the CMVP Coordination comments within the allotted timeframe, the CSTL  
 1029 must send an email justification to the CMVP identifying the reason for this delay at  
 1030 least two weeks prior to the drop date. The CSTL must include a timeline specifying the  
 1031 expected submission date for the CMVP's consideration. If no justification is received,  
 1032 the module will be dropped. A new submission could be sent once this module has been  
 1033 dropped but cost recovery would be applicable.

1034 6. A CSTL has been placed in a suspension status by NVLAP. Work in progress may be  
 1035 placed in a HOLD until the suspension is lifted. No new work is allowed to be  
 1036 submitted during a period of suspension.

1037 7. The report was sent back to the CSTL with Triage comments that must be addressed  
 1038 before the validation can continue. Once addressed, the CSTL sends an updated report,  
 1039 and the modules moves back to the state it was in prior. See [Section 4.1.1.2 Review](#)  
 1040 [pending](#) for more information on the Triage process.

1041 A module on HOLD will be reflected on the MIP List as “On Hold” with the date of status  
 1042 change. Once the HOLD is lifted, the MIP entry will return to its prior state and queue position.  
 1043 If an ECR is applicable, the ECR must be resolved, and any payment assigned must be paid  
 1044 before the HOLD can be removed.

#### 1045 4.3.5 Resubmission while in Review Pending

1046 An updated submission may be provided to the CMVP while in review pending if all the  
 1047 following rules are met:

- 1048 1. This is not to be used as a placeholder, and the initial submission must have been the  
 1049 intended version on the specified environment to be validated. Penalties (e.g., ECR, or  
 1050 drop the module queue position) may be applied if misused. Acceptable (non-  
 1051 exhaustive) examples include:
  - 1052 a. Code changes that strengthen the module’s conformance claim (e.g., improve the  
 1053 granularity of the module’s show version service, or reduce potential ambiguity  
 1054 with the module’s approved service indicators).
  - 1055 b. Changes under [Section 4.4.6](#) number 2 (a, b, and c).
- 1056 2. The updates must be allowed by and within the scope of the submission scenario, and  
 1057 full testing or regression testing may apply depending on the changes, following the  
 1058 requirements specified in [Section 7.1 Submission Scenarios](#).

1059 The updated submission will keep its place in the queue.

1060

#### 1061 4.3.6 Changes while in Coordination

1062 Changes during coordination for a FS or UPDT are permitted if all the following rules are met  
 1063 (subject to change, especially once additional [Section 7.1 Submission Scenarios](#) become  
 1064 available in Web Cryptik):

- 1065 1. Changes are limited to one or more of the following:
  - 1066 a. Quality / documentation updates to address CMVP checklist items or lessons  
 1067 learned from other module validations. Documentation improvements are  
 1068 encouraged to ensure accurate, high-quality reports and avoid ECR.
  - 1069 b. In direct response to CMVP comments.
  - 1070 c. Changes known at the time that would normally fit under: [CVE](#) or other

1071 vulnerability, [NSRL](#), [TRNS](#), [VUP](#), [VAOE](#), [OEUP](#)<sup>2</sup>, and/or [ALG](#). The  
 1072 requirements for these submission scenarios must be met per [Section 7.1](#)  
 1073 [Submission Scenarios](#) (e.g., limited changes, regression testing, CAVP/ESV  
 1074 testing, etc.).

1075 2. A detailed change summary needs to be provided to the CMVP for all changes that are  
 1076 outside 7.1 Submission Scenarios (this is expected to be part of the Comment document  
 1077 itself). For changes specific to the 7.1 Submission Scenarios, a separate Revalidation  
 1078 Change Document is required per [7.1.1](#).

1079 Notes:

- 1080 a. Updates to improve documentation is encouraged to ensure accurate, high-quality reports  
 1081 and avoid ECR.
- 1082 b. The review may be delayed for complexity (time incurred) depending on the impact of  
 1083 the changes.
- 1084 c. Post-validation (once supported by the CMVP), additional changes can be made using the  
 1085 revalidation scenarios per [Section 7.1](#) of this document.
- 1086 d. Code changes will impact compliance to AS04.13 due to new versioning.

#### 1087 4.3.7 Validation Deadline

1088 CMVP drops modules from the queue that have not completed the validation process within 2  
 1089 years of being placed in IN REVIEW status. Should the modules approach the 2-year deadline,  
 1090 CSTLs have the option to contact the CMVP for reconsideration; CMVP will consider factors  
 1091 that contribute to the delay (e.g. if the delay was not due to CSTL or vendor unresponsiveness /  
 1092 inadequacy in addressing CMVP comments in a timely and efficient manner). When the module  
 1093 is dropped, the vendor and lab must restart the validation process including paying a new cost  
 1094 recovery fee at the current rate. This applies to all submissions currently in the process as well as  
 1095 to new submissions.

#### 1096 4.4 Validation when Test Reports are not Reviewed by both Validation Authorities

1097 On rare occasions, laws from either country or other unusual circumstances prevent the release  
 1098 of product information outside its borders for specific products. In those occasions, both  
 1099 Validation Authorities will be advised of the circumstances, and the Validation Authority from  
 1100 that country will carry out the validation process on its own and present the certificate to the  
 1101 other Validation Authority for its signature (where applicable).

##### 1102 4.4.1 Controlled Unclassified Information

1103 If a CMVP test report is received from a CSTL and it is identified in the signed letter of

---

<sup>2</sup> Only permitted on a case-by-case basis with proper justification provided to the CMVP in advance of the resubmission. Considering the complexities of adding OEs, the CMVP may end up rejecting the proposal during Coordination and require adding OEs after the module has first been validated.

1104 affirmation that it is subject to the International Traffic in Arms Regulations<sup>3</sup> (ITAR), the  
1105 following CMVP programmatic guidance will be adhered to:

#### 1106 4.4.1.1 CMVP ITAR Guidance

- 1107 1. Report submission as specified in Web Cryptik applies and should include the following  
1108 changes from a normal submission:
  - 1109 a. A proprietary security policy [PDF] submitted in lieu of a non-proprietary  
1110 security policy.
  - 1111 b. Provide a signed letter of affirmation from the vendor stating the applicability  
1112 of ITAR to the submitted test report.
  - 1113 c. To satisfy binding of Cryptographic Algorithm Validation Certificates, (see [IG](#)  
1114 [2.3.A](#)), the test report must affirm that the CSTL has PDF images (front and  
1115 back) for any ITAR cryptographic algorithm validation certificates, where the  
1116 algorithm website will not have any detailed information.
  - 1117 d. The test report package is submitted only to NIST CMVP. The TID field will  
1118 be formatted as: TID-*nn-nnnn*-ITAR. The characters ITAR will replace the  
1119 field that was allocated for the CCCS TID.
  - 1120 e. Actual module names, version numbers, and vendor information will be  
1121 provided. This information will not be masked by dummy information.
- 1122 2. Report review
  - 1123 a. Each ITAR report will be reviewed by NIST reviewers.
- 1124 3. Certificate generation and posting
  - 1125 a. Certificates will be prepared by NIST only.
  - 1126 b. Certificates will be signed only by NIST. The CCCS signature field will be  
1127 marked as: Not Applicable – ITAR.
  - 1128 c. The NIST CMVP web page will only post the following information:  
1129 Certificate number, applicable FIPS standard, Status, Module Type,  
1130 Embodiment, Validation Date, Sunset Date and Overall Level. It will also  
1131 include the testing Lab and associated NVLAP Code.
  - 1132 d. The official certificate will be sent to the CSTL for presentation to the vendor.
- 1133 4. Re-validation
  - 1134 a. All re-validation changes will result in a new certificate sent to the CSTL for  
1135 presentation to the vendor since the web site will not have any identifiable  
1136 information.

---

<sup>3</sup>Example: 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.

1137           b. Report submission, report review, certificate generation and posting as outlined  
1138           above and following the submission requirements.

## 1139   **4.5   CMVP Fees<sup>4</sup>**

### 1140   4.5.1 Cost Recovery Program (CR & ECR)

1141   Fees are charged to the CSTL by NIST CMVP to offset the cost of the validation authority  
1142   activities performed by NIST CMVP. Cost Recovery (CR) fees are collected depending on the  
1143   submission scenario as listed in Submission Scenarios. Extended Cost Recovery (ECR) fees are  
1144   collected when the submission review exceeds the allotted resources and/or the submission  
1145   results in one of the categories in [3.2.8 Extended Cost Recovery](#). The ECR fee is billed separately  
1146   from any applicable CR fee.

1147   Fees charged by NIST as part of the cost recovery program are listed at:  
1148   <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees>.  
1149   Review of submissions will not begin until NIST CMVP receives confirmation that the invoice  
1150   has been paid. CR fees cannot be reimbursed after the submission has entered the In-Review  
1151   phase.

### 1152   4.5.2 NIST Payment Policy

1153   Only CSTLs with an active CRADA agreement can be invoiced. NIST CMVP maintains the  
1154   billing information for each CSTL. If the CSTL's information needs to be updated (e.g., [CSTL](#)  
1155   [relocation](#)), contact NIST CMVP. Upon receipt of the CSTL's submission or a request for an  
1156   invoice, NIST billing (a separate office of NIST) prepares an invoice and submits it to the  
1157   identified payee. For questions about methods of payments and associated handling fees contact  
1158   NIST Billing Information: 301-975-3880 or at [billing@nist.gov](mailto:billing@nist.gov). In the event a cost recovery  
1159   refund is warranted, the request must be directed to [cmvplab@nist.gov](mailto:cmvplab@nist.gov).

### 1160   4.5.3 Invoice for a Report Submission

1161   Currently, the CR process is initiated upon receipt of the report submission and typically adds an  
1162   average of 60 days to the validation process. The CR process can be initiated before the report  
1163   submission. In order to initiate the CR process, the CSTL must send an IUTA (IUT-Add) using  
1164   Web Cryptik indicating the correct number of modules, overall security level, and submission  
1165   type. The IUTA can be submitted without requesting that the module be placed on the IUT List.  
1166   The IUTA must be successfully processed by the NIST CMVP automated system. When the  
1167   submission is successfully processed, the CSTL will receive an automated response, "*Thank you*  
1168   *for your submission*".

1169   At any time after the CSTL receives the automated response to the IUTA, the CSTL has the  
1170   option to send an IUTB (IUT-Billing) to initiate the CR process before submitting the report.  
1171   When the IUTB is successfully processed, the CSTL will receive an automated response.

---

<sup>4</sup> CCCS does not levy any charges for the validation of cryptographic modules.

- 1172 Changes to the overall security level and submission type will not be accepted.
- 1173       o If the CSTL sends an IUTB and then needs to cancel the invoice, the CSTL must send  
1174       an IUTC (IUT-Cancel billing). When the IUTC is successfully processed, the CSTL  
1175       will receive the automated response.
- 1176       o Once the invoice has been paid, the payment may be refunded if the module submission  
1177       is dropped prior to the IN REVIEW stage.
- 1178       Only the vendor.json file is required for an IUTB or IUTC. For more information on this  
1179       process, see the Web Cryptik help and User Guide.
- 1180 Labs should note when the cost recovery process starts, no changes to the Security Level or  
1181 Submission Type will be accepted. In addition, if a report has not been received by 90 days after  
1182 the IUTB was accepted, the module will be moved to On Hold and removed from the IUT List.  
1183 The module can be automatically removed from On Hold and placed on the MIP List by sending  
1184 the report. If the lab chooses to not send an IUTB, the CR process will initiate upon receiving the  
1185 report submission.

#### 1186 4.6 Flaw Discovery Handling Process

1187 When a flaw is discovered in a **validated** cryptographic module and brought to the attention of  
1188 the CMVP Validation Authorities, the following actions will be taken:

- 1189       1. NIST, CCCS and the CSTL will investigate the allegation about the flaw, and  
1190       determine its impact on the validation;
- 1191       2. NIST and CCCS will decide whether the flaw requires the revocation of the  
1192       validation, a caveat be placed on the entry in the *Cryptographic Module Validation*  
1193       *List*, or no action;
- 1194       3. NIST and CCCS may notify NVLAP about the possible shortfall in the  
1195       CSTL's proficiency.

1196 The diagram found in Annex A outlines the flaw discovery handling process. There are several  
1197 ways for a flaw to be identified including a security-relevant CVE from the National  
1198 Vulnerability Database (NVD).

#### 1199 4.7 Historical or Revoked Validations

1200 **Historical** – Agencies may make a risk determination on whether to continue using this module  
1201 based on their own assessment of where and how it is used. For more details, please visit the  
1202 CMVP webpage: [https://csrc.nist.gov/Projects/cryptographic-module-validation-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules)  
1203 [program/validated-modules](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules)

1204 If the validation certificate is historical, it will appear on the *CMVP Validation List* with the  
1205 validation status *Historical*.

1206 Examples that may result in a FIPS 140 validation being made historical by the CMVP:

- 1207       • A validation implements cryptographic algorithm(s) in the approved mode that are no  
1208       longer approved (e.g., an algorithm transition date has passed that was identified as one

1209 that will move the module to the historical list per the CMVP [Programmatic Transitions](#)  
1210 webpage).

- 1211 • Sunset date as shown on the validation is reached.
- 1212 • A validation in bound to or embeds another validation that moved to the historical list  
1213 (e.g., due to being sunset or an algorithm transition).

1214 If an issue with a validation is discovered by the vendor or CSTL, the CMVP is to be notified of  
1215 the issue with a proposed schedule of when a correction will be submitted to the CMVP. The  
1216 CMVP will consider the severity of the issues, the proposed timeline for correction, and if the  
1217 issue was proactively requested (which is greatly encouraged/supported) when determining if the  
1218 validation should be revoked or made historical. E.g., the CMVP may decide to keep the  
1219 validation on the Active list until the revalidation submission is completed.

1220 The revalidation submission will either result in the same certificate being updated (i.e., no  
1221 further actions needed by the CMVP), or it will result in a new certificate number in which case  
1222 the original certificate may then be moved to the historical or revocation list. The CMVP may  
1223 move the module to the historical or revocation list if the corrections are not made in a timely  
1224 manner.

1225 **Revoked** - The module validation is no longer valid, and this certificate may not be referenced to  
1226 demonstrate compliance to FIPS 140-3.

1227 If the validation certificate is revoked, it will appear on the *CMVP Validation List* with the  
1228 validation status *Revoked*.

1229 Examples that may result in a FIPS 140 validation being revoked by the CMVP:

- 1230 a. Discovery of a security non-compliance or security flaw in a validated cryptographic  
1231 module (typically one that would require module code changes to correct).
- 1232 b. Discovery that the cryptographic module was validated using false information.
- 1233 c. A CVE is discovered, and the module has been updated to mitigate the CVE. The  
1234 module version with the CVE may be removed from the validation on the completion of  
1235 the CVE submission (see [7.1.11 CVE](#)).
- 1236 d. Significant documentation issues that have a security impact to the operator of the  
1237 module such as incorrect claims to:
  - 1238 ○ Any of the items in [7.8 Module definitions for same certificates](#),
  - 1239 ○ Module Caveat,
  - 1240 ○ Tested Configuration(s),
  - 1241 ○ Versions (i.e., Software, Firmware, or Hardware),
  - 1242 ○ Other CMVP documentation requirements (e.g., in IGs, MM, and SP 800-140  
1243 series) that have a security impact on the operator.

#### 1244 **4.8 Entropy Source Validation (ESV) Processes**

1245 In April 2022, the CMVP introduced a new submission process for entropy sources leading to

1246 standalone entropy source validation certificates. The validation certificates provide the  
 1247 assurance that a particular entropy source on a particular operating environment conforms to SP  
 1248 800-90B and associated IGs.

1249 Similar to ACVTS, the CMVP maintains two environments: a Demo ESVTS, and a Prod  
 1250 ESVTS. The Demo environment is for testing and becoming familiar with the platform. The  
 1251 Prod environment is for certification.

1252 Prod ESVTS is the only mechanism the CMVP allows on a new submission that requires a  
 1253 validation on an entropy source. Entropy source validation will no longer be accepted as part of a  
 1254 module submission (i.e., designated as ENT on the module certificate). Instead, the module  
 1255 submission must cite an existing entropy validation certificate. See Section 7.1.14 for additional  
 1256 information on ESV and ENT claims.

#### 1257 4.8.1.1 Entropy Source Validation Submissions

1258 To submit to ESVTS, a client must be used to interact with the server. The CMVP provides two  
 1259 clients for use: an HTML-based WebClient, and a Python client. Both have their advantages and  
 1260 features. It is encouraged that a lab is familiar with both options.

1261 Several files are expected to be included in the submissions. It is the best practice to have these  
 1262 ready before making the initial request to ESVTS. The minimum set of files are as follows:

- 1263 1. Entropy Assessment Report (EAR) – This file addresses the requirements in SP 800-  
 1264 90B and describes how the entropy source on the listed operating environments conforms  
 1265 to the standard and associated IGs.
- 1266 2. Public Use Document (PUD) – This file provides information to a user that may  
 1267 incorporate or use the entropy source within a cryptographic module.
- 1268 3. Data Collection Attestation (DCA) – This file addresses the SP 800-90B Section 3.2.4  
 1269 requirements. The document must contain the name of each operating environment tested  
 1270 in this manner and a signature from the vendor representative. This file is optional,  
 1271 depending on how the data was collected from the entropy source. It may also be attached  
 1272 to the EAR instead of provided separately.
- 1273 4. 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 e. Provide a signed letter of affirmation from the vendor stating the applicability of ITAR  
 1287 to the submitted report.
- 1288 f. 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 g. 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](mailto:christopher.celi@nist.gov).
- 1292 h. Comment responses go ONLY to [cmvpitar@nist.gov](mailto: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 i. 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 j. 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 k. 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 4.8.1.2 Entropy Source Validation Web Client

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.

#### 1319 4.8.1.3 Entropy Source Validation Python Client

1320 The Python Client provides a more automated way of submitting data to ESVTS. Requests may  
 1321 be made piecemeal when information becomes available. The user is expected to store the  
 1322 outputs from the tool. The tool automatically logs important information. The Python Client is  
 1323 controlled with JSON files to drive the functionality needed at the time. This allows a user to  
 1324 start making requests and pick them back up later. Configuration JSON files control if the

1325 Python Client is accessing Demo or Prod. The Python Client can be downloaded from the URL  
1326 indicated in the Entropy Source Validation Webpages (Section 4.8.3)

#### 1327 4.8.2 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 Any ESV submission that has substantial errors or requires significant additional review effort  
1339 by the validators (e.g., due to issues with quality or complexity) will be subject to a NIST ECR  
1340 (see HB 150-17 H.3.4.2).

#### 1341 4.8.3 Entropy Source Validation Webpages

1342 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)  
1343 [module-validation-program/entropy-validations](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations).

1344 The ESV Certificate List is available on CSRC. See [https://csrc.nist.gov/Projects/cryptographic-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations/search)  
1345 [module-validation-program/entropy-validations/search](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations/search).

1346 For access to the Python Client and ESVTS on Demo or Prod, see  
1347 <https://github.com/usnistgov/ESV-Server>.

### 1348 4.9 CMVP Webpages

1349 This section provides information about the CMVP program that can be found on the web.

#### 1350 4.9.1 Official CMVP Website

1351 The official CMVP website with all current publicly-available information on the CMVP is  
1352 <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program>. It can also be reached  
1353 through <https://nist.gov/cmvp>.

#### 1354 4.9.2 Cryptographic Module Validation Lists

1355 The official CMVP website can generate the following lists related to the validation of  
1356 cryptographic modules:

- 1357 • *Modules In Process* – A listing of the modules currently being reviewed by CMVP  
1358 and the review state of each module. For more information about the MIP List, see

- 1359 section 4.2.
- 1360 This list is updated as additional information is available. The validation process is a  
1361 joint effort between the CMVP, the CSTL and the vendor and therefore, for any given  
1362 module, the action to respond could reside with the CMVP, the lab or the vendor. This  
1363 list does not provide granularity into which entity has the action.
- 1364 • *Implementation Under Test* – A listing of the modules currently being tested at the  
1365 CSTL. This list is provided by the CSTLs and includes module name, vendor, FIPS  
1366 140-2 or FIPS 140-3, and the date when added to the list.
- 1367 This list is updated as information is available. The IUT is under the control of the  
1368 CSTL and the vendor. The CMVP is not aware of the submission schedule for these  
1369 modules under testing.
- 1370 • *Cryptographic Module Validation Search can be found at:*  
1371 [https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search)  
1372 [modules/Search](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search)
- 1373 - A basic search supports a single overall list or a list resulting from a  
1374 combination of vendor, module name, or certificate number. The basic search  
1375 only addresses active modules.
  - 1376 - An advanced search will generate a single list with the following options:
    - 1377 • Certificate Number:
    - 1378 • Vendor:
    - 1379 • Module Name:
    - 1380 • Standard: (FIPS 140-1, FIPS 140-2, or FIPS 140-3)
    - 1381 • Module Type:
    - 1382 • Validation Status: (Active, Historical, or Revoked)
    - 1383 See the following web page for additional information
    - 1384 [https://csrc.nist.gov/Projects/cryptographic-module-validation-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules)  
1385 [program/validated-modules](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules)
    - 1386 • Embodiment:
    - 1387 • Year Validated:
    - 1388 • Overall Security Level:
    - 1389 • Algorithm:
    - 1390 • Allowed Algorithms:
    - 1391 • Tested Configuration:
    - 1392 • Caveat:
    - 1393 • Hardware Versions:
    - 1394 • Software Versions:
    - 1395 • Firmware Versions:
    - 1396 • Lab:
- 1397 The search is updated when new validation certificates are posted to the website.  
1398 Only the current validation information is shown, however, changes are indicated  
1399 in the validation history.
- 1400 The lists are being improved as needs and time allows, so that more information  
1401 than indicated here may be available from these sources before the next update of

1402 this document.

### 1403 4.9.3 CMVP Certificate Page Links

1404 Once the validation is identified, the information displayed typically includes vendor  
1405 information, module information, and required caveats. For each certificate there are also several  
1406 links from these pages that may be useful. These are described below.

#### 1407 4.9.3.1 Security Policy

1408 This link is connected to the security policy that is the vendor provided summary of the  
1409 capabilities and security information of the module in a PDF format. The file is created under the  
1410 agreement from the vendor and is available from the CMVP website.

#### 1411 4.9.3.2 Consolidated Validation Certificate

1412 This link is connected to a list of certificates that were issued for the month of interest. It  
1413 provides summary information that is accurate at the time of signing. For the latest module  
1414 information, please refer to the certificate page. The file is created by CMVP and is from the  
1415 CMVP website. Recent validations may not have this link available until the consolidated  
1416 certificate process can be completed.

#### 1417 4.9.3.3 Vendor Link

1418 This link is provided by the vendor to CMVP. The vendor is responsible for the accuracy of the  
1419 link and the content. The CMVP does not endorse the views expressed or the information  
1420 presented in the directed link, nor does it endorse any commercial products that may be  
1421 advertised or available at the directed link.

#### 1422 4.9.3.4 Vendor Product Link

1423 The purpose of this web link is for vendors to provide a concise listing of known products which  
1424 incorporate their validated cryptographic module or, if the cryptographic module is a standalone  
1425 product, additional relevant information about the product. The CMVP hopes that this link will  
1426 make it easier for potential customers and users to identify products that use validated  
1427 cryptographic modules.

1428 The link in the certificate details page is to a vendor provided URL that is vendor created and  
1429 vendor maintained. The provision of this Vendor Product Link by the vendor is optional. The  
1430 CMVP does not endorse the views expressed or the information presented in the directed link  
1431 nor does it endorse any commercial products that may be advertised or available at the directed  
1432 link. Press releases are not accepted.

#### 1433 4.9.3.5 Algorithm Certificates

1434 Links to the CAVP validation certificate for the approved algorithms used in the module are

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

#### 1438 4.9.3.6 Validation History

1439 The initial validation and all updates are shown along with the CSTL responsible. The validation  
1440 shown includes all updates and is considered the official validation. If information concerning a  
1441 revalidation is needed, contact the CSTL indicated on the validation certificate.

#### 1442 4.9.4 Usage of FIPS 140-3 Logos

1443 Once validation is achieved CMVP will forward through the CSTL to the Vendor instructions  
1444 about the use of the NIST FIPS 140-3 logo. Vendors who use validated modules in their products  
1445 may also request use of the NIST FIPS 140-3 Logo. The request instructions and use  
1446 requirements is available from the CMVP web site: [https://csrc.nist.gov/Projects/cryptographic-  
1447 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  
1448 [cmvp@nist.gov](mailto:cmvp@nist.gov).

## 1449 **5 CMVP and CAVP Programmatic Metrics Collection**

1450 This section provides an overview of the CMVP and CAVP Programmatic Metrics Collection  
1451 and a description of the collection and reporting processes of the CMVP metrics.

### 1452 **5.1 Overview**

1453 The CMVP Programmatic Metrics Collection process is intended to document the quality  
1454 performance of the testing and validation processes of the CMVP and to allow the program to  
1455 evaluate its relevance within the government. To achieve these objectives various metrics are  
1456 collected through the testing and validation processes of the CSTLs and the CMVP. These  
1457 metrics are intended to identify general programmatic trends and not to measure individual  
1458 CSTL or vendor performances.

### 1459 **5.2 Confidentially of the Collected Metrics Data**

1460 The CMVP considers the data collected and reported by the individual CSTLs as proprietary.  
1461 CMVP makes every effort to anonymize the information by sampling only larger data sets and  
1462 combining them without tracking information. The statistical information derived from the  
1463 collected data is considered to be non-proprietary.

### 1464 **5.3 Collected Metrics**

1465 With the migration to FIPS 140-3 and the changes in the collection tools, the CMVP are  
1466 currently reevaluating the methods used to collect useful metrics. Though the program will likely  
1467 follow much of the previous procedures, it is not possible at this time.

## 1468 6 Test Tools

1469 This section covers the testing tools CSTLs are expected to utilize in the testing and reporting of  
 1470 validation submissions. Where applicable, the title of the person responsible for the update  
 1471 and/or maintenance of the document is identified.

### 1472 6.1 Web Cryptik

1473 Web Cryptik is a required tool for the completion of module testing, and generation of  
 1474 documents that must be included in a formal submission from the CST. The Web Cryptik tool is  
 1475 to be used to record details of the cryptographic module being tested, the specific testing  
 1476 performed, and the results of the validation testing. It is also to be used to create, among other  
 1477 documents, the FIPS 140 validation test report and draft certificate. Information about new  
 1478 features, enhancements, and bug fixes are provided with each release of the tool in the Web  
 1479 Cryptik User Guide.

1480 Most submissions to CMVP are done through the use of Web Cryptik. The Web Cryptik User  
 1481 Guide provides a summary table of the submissions supported by Web Cryptik and files that  
 1482 must be included with the submission.

1483 **Responsible Individual:** NIST CMVP Program Manager.

### 1484 6.2 Suggested Tools for Physical Testing

1485 As indicated in HB 150-17 Section B.6.4.2, a CSTL must meet the minimum hardware and  
 1486 software requirements for physical security testing. The CSTL can determine which tools to use  
 1487 to meet the requirements. All measurement equipment used to meet specific criteria in the  
 1488 conformance testing must have a valid calibration certificate from a separate accredited  
 1489 calibration laboratory. All equipment with storage capabilities must meet CSTL security  
 1490 policies. Personal equipment is prohibited for use in testing.

1491 Below are some examples:

- 1492 X-Acto or Utility "Type" knives (including various blades)
- 1493 Strong artificial light source (Wavelength range of 400nm to 750nm)
- 1494 Magnifying glass
- 1495 Dremel "Type" Rotary Tool (including accessory bits: cutting, grinding, drilling, carving,  
 1496 etc.)
- 1497 Jeweler's screwdrivers (e.g., flat, phillips, robertson, torx, hex key)
- 1498 Dentist "Type" Instruments (e.g., picks and mirrors)
- 1499 Razor Saw
- 1500 Small pliers (e.g., needle nose, standard nose, long nose, curved nose, side cutters)
- 1501 Hammer
- 1502 Chisels
- 1503 Fine (small) files
- 1504 Heat Gun or Heat Source
- 1505 Spray Coolant
- 1506 Digital camera (personal phones are not acceptable)

- 1507 Digital scanner
- 1508 Printer
- 1509 ANSI C Compiler
- 1510 Debugger or binary editor
- 1511 Microsoft Office Professional
- 1512 Adobe Acrobat Standard
- 1513 Personal protection equipment for chemical testing (e.g., goggles, gloves)
- 1514
- 1515 The equipment below may require calibration if used to measure to a reference:
- 1516
- 1517 Volt-Ohm-Milliammeter (VOM) or Digital Multimeter (DMM)
- 1518 Variable Power Supply
- 1519 Digital Storage Oscilloscope and/or Logic Analyzer
- 1520 Temperature Chamber

## 1521 7 CMVP General Testing and Reporting Guidance

1522 In order for CMVP to manage the program more efficiently, additional testing requirements are  
1523 addressed below. Several of the issues that were under section G of the FIPS 140-2  
1524 Implementation Guidance are presented in this section. This guidance does not change the  
1525 cryptographic module requirements of ISO/IEC 19790:2012 but may impact ISO/IEC  
1526 24759:2017 documentation and testing requirements.

### 1527 7.1 Submission Scenarios

1528 An updated version of a previously validated cryptographic module can be considered for a  
1529 *revalidation* rather than a *full validation* depending on the extent of the modifications from  
1530 the previously validated version of the module. (Note: the updated version may be, for  
1531 example, a new version of an existing cryptographic module or a new model based on an  
1532 existing model.)

#### 1533 7.1.1 Requirements for all revalidations

1534 For any revalidation, the vendor is responsible for reviewing all FIPS 140-3 requirements  
1535 and making sure any change has been addressed throughout the module requirements and  
1536 that proper documentation has been completed and submitted to the CSTL. The CSTL is  
1537 responsible for an independent evaluation of the impacts throughout the module  
1538 requirements for any change and performs any testing needed prior to submission. The  
1539 CSTL **shall** address all affected TEs and the CSTL's assessment. The details **shall** be  
1540 included in an updated Web Cryptik package with a summary of the changes listed in the  
1541 Revalidation Change Document (<https://csrc.nist.gov/projects/cmvp/sp800-140b>).

1542 For all revalidations, the Web Cryptik package **shall** include all information required by  
1543 that revalidation scenario. The ZIP file and files within the ZIP file **shall** follow the  
1544 requirements in the Web Cryptik User's Guide and be submitted to the CMVP using the  
1545 specified data protection methods. Additional documentation may be required if CMVP  
1546 guidance requiring the additional documentation has been published since the module's  
1547 original validation.

1548 All scenarios **shall** be processed and submitted to the CMVP by a CSTL.

1549 If a CSTL has been contracted to perform a revalidation for a validated module for which the  
1550 CSTL did not perform the original testing on the base module:

- 1551 a. The vendor **shall** provide the CSTL with the design documentation and  
1552 implementation (including source code, HDL, etc.) of the base validated module and  
1553 of the module that has been updated.
- 1554 b. The vendor **shall** provide the CSTL with the latest Security Policy as shown on the  
1555 base module's most recent certificate (this includes the JSON files and information  
1556 necessary to generate the Security Policy for SP 800-140Br1-compliant base  
1557 modules).

- 1558 c. The vendor **shall** provide the CSTL with the latest base module validation report  
 1559 (a.k.a. Test Report) for the following revalidation scenarios: NSRL, ALG, UPDT,  
 1560 CVE and TRNS. This is to ensure the new CSTL has the original tests to confirm if  
 1561 regression testing is necessary in addition to the minimum required by that  
 1562 revalidation scenario.
- 1563 d. The vendor **shall** provide the CSTL with the latest base module physical test report  
 1564 (a.k.a. PTR) for the following revalidation scenarios: NSRL, UPDT, CVE, TRNS and  
 1565 PHYS. This is to ensure the new CSTL can determine if physical testing was  
 1566 impacted (e.g., changes to the physical enclosure or changes to firmware that controls  
 1567 the physical response logic).
- 1568 e. The CSTL **shall** determine that the provided base documentation and implementation  
 1569 is identical to the base validated module.
- 1570 f. The CSTL **shall** examine each modification and confirm that the change is  
 1571 appropriate for the submission type (e.g., non-security relevant for NSRL).
- 1572 g. The CSTL **shall** determine that no other modifications, including unintentional, have  
 1573 been made to the base module apart from what is permitted by the revalidation  
 1574 scenario.
- 1575 h. The CSTL submissions **shall** meet all requirements of the revalidation scenario.
- 1576 i. The CSTL submission **shall** indicate which submission scenario is applicable and a  
 1577 summary of associated changes in the Change Document.
- 1578 j. The CSTL **shall** use the Change Document format for listing the certificate  
 1579 information as required by each revalidation scenario.
- 1580 k. The CSTL **shall** submit, at a minimum, what is listed below as required by the  
 1581 revalidation scenario.

1582 Below are the twelve possible FIPS 140-3 submission scenarios: Full Submission (FS), Vendor  
 1583 Update (VUP), Vendor Affirmed Operational Environment (VAOE), Non-Security Relevant  
 1584 (NSRL), Algorithm Update (ALG), Operational Environment Update (OEUP), Rebrand  
 1585 (RBND), Port Sub Chip (PTSC), Update (UPDT), Common Vulnerabilities and Exposures  
 1586 (CVE), Algorithm Transition (TRNS), and Physical Enclosure (PHYS).

1587 See [section 7.1.14](#) for a summary table and submission process for each of these  
 1588 submission scenarios, and [section 7.1.15](#) for additional comments.

### 1589 7.1.2 Full Submission (FS)

1590 The first time a new software, firmware, hardware, or hybrid module is submitted for validation.  
 1591 The module **shall** meet all applicable requirements at the time of submission.

1592 If modifications are made to hardware, software, or firmware components that do not meet any  
 1593 of the below revalidation criteria, then the cryptographic module **shall** be considered a new  
 1594 module and **shall** undergo a full validation testing by a CSTL and submitted as a FS.

## 1595 7.1.2.1 Interim Validation

1596 This is a temporary measure to shorten the queue and expand the active validations. These  
 1597 validations are valid for two years only but can be converted to a normal full validation (with a  
 1598 5-year validation date) on the completion of an additional conversion/submission compliant to  
 1599 SP 800-140Br1.

1600 Interim validations currently can only be modified under VUP, VAOE, NSRL, and CVE  
 1601 (described below).

1602 The main difference from a normal validation is that for interim validations, the CMVP depends  
 1603 more on the CSTL submission with less CMVP oversight. For more information see the CMVP  
 1604 webpage: [https://csrc.nist.gov/projects/cryptographic-module-validation-program/programmatic-](https://csrc.nist.gov/projects/cryptographic-module-validation-program/programmatic-transitions)  
 1605 [transitions](https://csrc.nist.gov/projects/cryptographic-module-validation-program/programmatic-transitions).

## 1606 7.1.3 Vendor Update (VUP)

1607 Administrative updates (e.g., updating vendor contact information, grammatical Security Policy  
 1608 corrections).

## 1609 7.1.4 Vendor Affirmed Operational Environment (VAOE)

1610 Security policy change of vendor affirmed OEs (see Management Manual 7.9 *Vendor or User*  
 1611 *Affirmation of Modules*).

## 1612 7.1.5 Non-Security Relevant (NSRL)

1613 Modifications are made to hardware, software or firmware components **that do not affect any**  
 1614 **FIPS 140-3 security relevant items**. Per [IG 2.4.A](#), “the term *security* is not defined in the Terms  
 1615 and Definitions, but, within the scope of FIPS 140-3, is determined based on the Section 6  
 1616 Functional Security Objectives, and the specific Section 7 Security Requirements derived from  
 1617 those objectives”. The CSTL is responsible for identifying the documentation that is needed to  
 1618 determine whether a revalidation is sufficient, and the vendor is responsible for submitting the  
 1619 requested documentation to the CSTL. Documentation may include a previous validation report,  
 1620 design documentation, source code, source code difference evidence, FSM, security policy  
 1621 differences, etc.

1622 The CSTL **shall**:

- 1623 a. review and independently verify the accuracy of the vendor-supplied documentation and  
 1624 identify any additional documentation necessary to confirm the applicability of this  
 1625 revalidation scenario.
- 1626 b. determine additional testing as necessary to confirm that FIPS 140-3 security relevant  
 1627 items have not been affected by the modification.
- 1628 c. identify the assertions affected by the modification and **shall** perform the tests associated  
 1629 with those assertions. This will require the CSTL to:
- 1630 i. Review the COMPLETE list of assertions applicable to the module,

- 1631           ii. Identify, from the previous validation report, the assertions that have been  
1632           affected by the modification,
- 1633           iii. Identify additional assertions that were NOT previously tested but should now be  
1634           tested due to the modification, and
- 1635           iv. Review assertions where specific Implementation Guidance (IG) was provided at  
1636           the time of the original validation to confirm that the module still meets the IG as  
1637           it existed at the time of the original validation.
- 1638           d. Perform tests identified in b and c above (expected to at least include AS04.13 to reflect  
1639           the new version(s) as a result of the code changes) on all new version(s) listed on the  
1640           module’s certificate on at least one configuration of one module as defined per the  
1641           module count guidance under “[MIS Field Descriptions](#)”. Additionally for  
1642           software/firmware/hybrid modules, tests much be done on at least one listed OE. This  
1643           assumes the new versions compile to the same binary across all modules and  
1644           configurations. If new versions compile to different binaries, then each binary must be  
1645           tested separately.
- 1646           i. E.g., a hardware validation has two ‘base’ modules (i.e., P/N 10 and P/N 20) that  
1647           map to the following firmware components: P/N 10 uses firmware components  
1648           1.0 and 2.0, and P/N 20 uses firmware components 1.1, 2.0, and 3.0 (note, the  
1649           same firmware component, 2.0, is shared between both ‘base’ modules). If NSRL  
1650           changes were made to firmware component 2.0 (now version 2.1) but no changes  
1651           were made to firmware components 1.0, 1.1 and 3.0, it is sufficient for the CSTL  
1652           to test either: 1) P/N 10 using 1.1 and 2.1, or 2) P/N 20 using 1.0, 2.1, and 3.0.  
1653           This assumes firmware component 2.1 compiles to the same binary for P/N 10  
1654           and P/N 20. If not, P/N 10 and P/N 20 would each need to be separately tested.
- 1655           ii. If regression testing is not performed on some versions, then those **shall** be  
1656           removed from the module’s certificate. The CSTL **shall** provide justification on  
1657           why regression testing is not necessary for the untested configurations and OEs.  
1658           With proper justification, these may remain on the module’s certificate. Without  
1659           proper justification or regression testing, untested configurations or OEs **shall** be  
1660           removed from the module’s certificate.

1661 NSRL code changes (“limited” or not) would NOT require retesting CAVP certificates (even if  
1662 applicable per the CAVP [FAQ GEN.9](#)), since changes are non-security relevant and verified by  
1663 the CSTL as having no impact to the algorithm implementations or how it meets CAVP testing.  
1664 CAVP [FAQ GEN.11](#) may be leveraged to update the CAVP versioning information if changes  
1665 are made outside the algorithm boundary but still impact the versioning on the CAVP certificate  
1666 (e.g., the CAVP versioning reflects the module boundary rather than the algorithm boundary).

1667 The CSTL may send the CMVP a [Request For Guidance](#) to confirm their analysis on the non-  
1668 security relevant changes prior to submission, which is expected to address at least the following  
1669 questions:

- 1670           1. What changes are being proposed?

- 1671 2. What is the justification that each change is considered non-security relevant? E.g.,  
1672 changes are NOT to any items from [7.8 Module definitions for same certificates](#) or other  
1673 areas that affects how the module meets the security objectives and requirements of FIPS  
1674 140-3.

#### 1675 7.1.6 Algorithm Update (ALG)

1676 Post validation, approved security relevant functions or services for which CAVP testing was not  
1677 available (or vendor affirming was still permitted per the CMVP/CAVP transition schedule) at  
1678 the time of submission to the CMVP for validation are now CAVP-tested and are being  
1679 submitted for inclusion as an approved function or service. The CSTL is responsible for  
1680 identifying the documentation that is needed to determine whether a revalidation is sufficient,  
1681 and the vendor is responsible for submitting the requested documentation to the CSTL.  
1682 Documentation may include a previous validation report and applicable CMVP rulings, design  
1683 documentation, source code, security policy differences, etc. Code or configuration changes are  
1684 not permitted under this revalidation scenario. For example, if self-tests are required for  
1685 approved algorithms, the module must already support these self-tests. In essence, this means  
1686 that ALG can only be used when a previously vendor affirmed or allowed algorithm now has  
1687 CAVP testing available and already meets the algorithm requirements (e.g., self-tests) and  
1688 module requirements (e.g., approved service indicator).

1689 The CSTL **shall**:

- 1690 a. review and independently verify the accuracy of the vendor-supplied documentation and  
1691 identify any additional documentation necessary to confirm the applicability of this  
1692 revalidation scenario.
- 1693 b. identify the assertions affected by the modification and **shall** perform the tests associated  
1694 with those assertions. This will require the CSTL to:
- 1695 i. Review the COMPLETE list of assertions applicable to the module,
  - 1696 ii. Identify, from the previous validation report, the assertions that have been  
1697 affected by the modification,
  - 1698 iii. Identify additional assertions that were NOT previously tested but should now be  
1699 tested due to the modification, and
  - 1700 iv. Review assertions where specific Implementation Guidance (IG) was provided at  
1701 the time of the original validation to confirm that the module still meets the IG as  
1702 it existed at the time of the original validation, except for IGs related to the newly  
1703 tested algorithm where the latest IGs **shall** be met.

#### 1704 7.1.7 Operational Environment Update (OEUP)

1705 No changes to the module with an addition, modification, or deletion of tested operational  
1706 environments (OEs). Purely deleting OEs can be done as a NSRL, but deleting can be done  
1707 within an OEUP if also adding and/or modifying OEs. This **shall** require CAVP-testing the  
1708 algorithm validations on the new/modified OEs. If an entropy source assessment is applicable

1709 per [IG 9.3.A](#), ESV(s) to cover all new/modified OEs and/or platforms **shall** be submitted and  
 1710 validated separately prior to submission. The CSTL **shall** perform the full regression test suite  
 1711 shown on the [CMVP website](#).

1712 The only time code changes are allowed as part of an OEUP is if they are non-security relevant  
 1713 and *necessary* to correctly run the module on the new/modified OE (e.g., compilation flags or  
 1714 configuration options that need to be updated). No other changes are permitted (even to  
 1715 incorporate other non-security relevant changes such as bug fixes). In Web Cryptik, this may be  
 1716 captured as a checkbox under the OEUP submission scenario (e.g., the CSTL selects “Limited  
 1717 NSRL”).

1718 Upon re-testing and validation, the CMVP provides the same assurance as the original OE(s) as  
 1719 to the correct operation of the module on the new/modified OS(s) and/or OE(s). The  
 1720 new/modified OS and/or OE will be added to the module’s validation entry.

1721 As a potential alternative to an OEUP, module vendors and users may take advantage of the  
 1722 porting provisions explained in [7.9 \(Vendor or User Affirmation of Modules\)](#) of this document.

#### 1723 7.1.8 Rebrand (RBND)

1724 This scenario applies if there are no modifications to a module and the new module is a re-  
 1725 branding of an already validated Original Equipment Manufacturer (OEM) module. The CSTL  
 1726 **shall**:

- 1727 1. determine that the re-branded module is identical to the OEM module (n.b. this  
 1728 requirement applies equally to open source and non-open-source modules).
- 1729 2. include the OEM’s written approval for re-branding in the submission package which  
 1730 **shall** note the terms of permission (e.g., subsequent addition of OEs, possible re-use of  
 1731 CAVP certificates, entropy, non-security relevant changes, remediation of CVE, whether  
 1732 a rebrand of a rebrand is acceptable, etc.) including who owns/controls the codebase and  
 1733 is responsible for updates to it post validation. E.g., if these terms do not explicitly allow  
 1734 a vendor to further rebrand the OEM module, then a rebrand of that rebranded module is  
 1735 not permitted unless written permission is granted by the OEM.
- 1736 3. (for modules containing any open-source licensed code) ensure the open-source licensing  
 1737 requirements are met (e.g., any required notices are contained in the Security Policy).

1738 A RBND **shall** include at least one OE from the original validation and cannot add new OEs.  
 1739 With proper OEM permissions, a RBND followed by an OEUP can accomplish rebranding a  
 1740 module on different OEs.

1741 The only time it is allowed to combine a RBND with other scenarios is as follows:

- 1742 a. A RBND may be combined with a PHYS only if physical changes are necessary to  
 1743 correctly rebrand the module. For example, if the paint or coating on the hardware of the  
 1744 rebranded module is changed to reflect the new company's color schemes, and/or to  
 1745 change the vendor and product names on the enclosure. In Web Cryptik, this may be  
 1746 captured as a checkbox under the RBND submission scenario (e.g., the CSTL selects  
 1747 “PHYS”).  
 1748

- 1749        b. The only time code changes are allowed as part of a RBND is if they are necessary to  
 1750        correctly rebrand the module (e.g., to display the new module name/version/logo, or to  
 1751        use the new vendor's color schemes/visual aesthetics). No other changes are permitted  
 1752        (even to incorporate other non-security relevant changes such as bug fixes). In Web  
 1753        Cryptik, this may be captured as a checkbox under the RBND submission scenario (e.g.,  
 1754        the CSTL selects “Limited NSRL”).  
 1755
- 1756        c. A RBND is almost guaranteed to be combined with a VUP to address the vendor changes  
 1757        so this will not be separately selectable in Web Cryptik.  
 1758
- 1759        d. A vendor is expected to have permission to reuse the OEM’s CAVP certificates.  
 1760        Therefore, changes to CAVP certificate information are NOT permitted as part of a  
 1761        RBND (but depending on the permissions, may be part of a post-RBND revalidation).  
 1762

1763        The CSTL **shall** provide an updated security policy which is technically identical to the  
 1764        originally validated security policy and describes the re-branded module.

#### 1765        7.1.9 Port Sub Chip (PTSC)

1766        A sub-chip cryptographic subsystem that was previously validated in a single-chip (see [IG 2.3.B](#))  
 1767        can be ported to other single-chip constructs as a PTSC submission to the CMVP. The following  
 1768        is applicable to validate this new single-chip module:

- 1769        • The CSTL **shall** verify that there are no security relevant changes in the sub-chip  
 1770        cryptographic subsystem;
- 1771        • If an entropy source is contained within the sub-chip cryptographic subsystem, ESV(s) to  
 1772        cover all new single-chip environments **shall** be submitted and validated separately prior  
 1773        to submission;

1774        **Note 1:** An ESV may not be required, if the entropy is collected outside the sub-chip  
 1775        cryptographic subsystem, depending on changes to the entropy source or the  
 1776        subsystem housing it. Please refer to [IG 9.3.A](#) and [IG D.J](#) for details on applicable  
 1777        caveats and entropy estimates.

1778        **Note 2:** Single chip embodiments may implement an ESV or a DRBG linked to a dedicated  
 1779        entropy source inside the physical boundary. Such cases may be implemented (a)  
 1780        inside the sub-chip cryptographic subsystem or (b) in two or more sub-chip  
 1781        cryptographic subsystems. The case (b) represents multiple disjoint sub-chip  
 1782        cryptographic subsystems (see 3 of [IG 2.3.B](#)).

- 1783        • Approved security functions **shall** be retested and validated by the CAVP if implemented  
 1784        in a soft circuitry core recompiled in a different part configuration. In Web Cryptik, this  
 1785        case is expected to be captured as a checkbox under the PTSC submission scenario (e.g.,  
 1786        the CSTL selects “CAVP Testing Redone”).

1787        **Note 3:** If the original algorithm testing was performed as stated in the [Management Manual](#)  
 1788        Section 7.3 – *Testing using Emulators and Simulators* in a module simulator, and there is  
 1789        no change to the soft-core, no additional algorithm testing is required.

- 1790
- 1791
- 1792
- 1793
- 1794
- 1795
- 1796
- 1797
- 1798
- 1799
- 1800
- 1801
- 1802
- 1803
- 1804
- 1805
- 1806
- 1807
- 1808
- 1809
- 1810
- 1811
- Full regression testing (see FIPS 140-3 [Resources page](#)) **shall** be performed on the new sub-chip cryptographic subsystem after fabrication (transformation of the HDL to a gate or physical circuitry representation);
  - **ISO/IEC 19790:2012** Section 7.3 **shall** be addressed for the new single-chip module for all Security Levels within this Section.
  - **ISO/IEC 19790:2012** Section 7.7 **shall** be addressed for the new single-chip module at Security Level 1.
  - **ISO/IEC 19790:2012** Sections 7.11.2 and 7.11.9 **shall** be addressed for the new single-chip module for all Security Levels within this Section.
  - A new Security Policy **shall** be provided for the new single-chip module.
  - Versioning information on the new certificate **shall** be provided for:
    - the new physical single-chip,
    - non-security relevant single-chip functional subsystem firmware if applicable,
    - the sub-chip cryptographic subsystem soft and hard circuitry cores (which are unchanged from the original validation), and
    - the associated firmware.
  - The only time code changes are allowed as part of an PTSC is if they are non-security relevant and necessary to correctly run the module on the new/modified single chip environment (e.g., compilation flags or configuration options that need to be updated). No other changes are permitted (even to incorporate other non-security relevant changes such as bug fixes). In Web Cryptik, this may be captured as a checkbox under the PTSC submission scenario (e.g., the CSTL selects “Limited NSRL”).

#### 1812 7.1.10 Update (UPDT)

1813 Modifications are made to hardware, software or firmware components **that affect some of the**

1814 **FIPS 140-3 security relevant items**. Per [IG 2.4.A](#), “the term *security* is not defined in the Terms

1815 and Definitions, but, within the scope of FIPS 140-3, is determined based on the Section 6

1816 Functional Security Objectives, and the specific Section 7 Security Requirements derived from

1817 those objectives”. An updated cryptographic module can be considered in this scenario if less

1818 than a 30% of security changes were made to the module. Security changes include impacts to:

1819 approved / allowed security functions/algorithms, SSPs, approved security services, self-tests,

1820 and security states within the FSM. None of these, assessed individually, can exceed 30% of

1821 changes. The individual ratios for each of these **shall** be provided to the CMVP within the

1822 Revalidation Change Document (e.g., 2 approved security services out of 10 total results in 20%

1823 change).

1824 The CSTL is responsible for identifying the documentation that is needed to determine whether a

1825 revalidation is sufficient, and the vendor is responsible for submitting the requested

1826 documentation to the CSTL. Documentation may include a previous validation report and

1827 applicable CMVP rulings, design documentation, source code, source code difference evidence,

1828 FSM etc.

1829 The CSTL **shall**:

- 1830 a. provide a summary of the changes and rationale of why this meets the <30% guideline.  
 1831 The CMVP upon review, may determine that the changes are >30% and **shall** be  
 1832 submitted as an FS.
- 1833 b. review and independently verify the accuracy of the vendor-supplied documentation and  
 1834 identify any additional documentation necessary to confirm the applicability of this  
 1835 revalidation scenario.
- 1836 c. identify the assertions affected by the modification and **shall** perform the tests associated  
 1837 with those assertions. This will require the CSTL to:
- 1838 i. Review the COMPLETE list of assertions applicable to the module,
  - 1839 ii. Identify, from the previous validation report, the assertions that have been  
 1840 affected by the modification,
  - 1841 iii. Identify additional assertions that were NOT previously tested but should now be  
 1842 tested due to the modification, and
  - 1843 iv. Review assertions where specific Implementation Guidance (IG) was provided to  
 1844 confirm that the module meets all current applicable IGs.

1845 In addition to the tests performed against the affected assertions, the CSTL **shall** perform the  
 1846 regression test suite shown on the [CMVP website](#).

1847 The UPDT can also be used to for resetting the module’s sunset date when a module has not  
 1848 changed, provided the above requirements are met.

1849 UPDT can be combined with any submission scenario(s) except VUP or VAOE. In Web Cryptik,  
 1850 it is expected that in this case, the CSTL selects the appropriate checkbox(s) after choosing the  
 1851 UPDT submission scenario.

#### 1852 7.1.11 Common Vulnerabilities and Exposures (CVE)

1853 A CSTL has been contracted to perform a revalidation for a module on which the vendor has  
 1854 made FIPS 140 security-relevant changes in response to one or more CVEs (Common  
 1855 Vulnerability and Exposure). For more information about CVEs please see  
 1856 <https://cve.mitre.org/>.

1857 This revalidation scenario provides the vendor with a means to quickly fix, test, and revalidate a  
 1858 module subject to a *security-relevant CVE*<sup>1</sup> while at the same time providing assurance that the  
 1859 module still meets the FIPS 140-3 standard. If a CVE does not require security-relevant changes  
 1860 to address it, then the vendor may pursue an NSRL revalidation.

1861 To complete a Scenario CVE revalidation:

- 1862 a. The CSTL **shall** determine that security relevant changes to the module are only  
 1863 to correct the vulnerability disclosed in the CVE. Other changes are permitted if  
 1864 only directly impacted by the CVE change (e.g., addressing the CVE may require  
 1865 changing the version number, and that requires the show version service be  
 1866 updated). In WebCryptik, this may be captured by selecting “Limited NSRL”  
 1867 checkbox after choosing the CVE submission scenario.

- 1868           b. The CSTL **shall** examine each modification and confirm that the change does not  
1869           conflict with the requirements of FIPS 140-3.
- 1870           c. The CSTL **shall** determine that no other modifications have been made.
- 1871           d. The CSTL **shall** identify the assertions affected by the security-relevant  
1872           modification and **shall** perform the tests associated with those assertions.
- 1873           e. The vendor is not required to address IGs that have been published since  
1874           submission of the original module, besides following the continual guidance of [IG](#)  
1875           [11.A](#) (CVE Management).
- 1876           f. If the fix to address the CVE is in the scope of an algorithm implementation (e.g.,  
1877           involves a change that requires retesting per the CAVP), then this algorithm **shall**  
1878           be CAVP tested again to obtain a new CAVP certificate with the new module  
1879           version. In this case, the CSTL selects the “CAVP Testing Redone” sub-option in  
1880           Web Cryptik after choosing the CVE submission scenario.

1881           In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the  
1882           predefined regression tests shown on the [CMVP website](#), under CVE.

1883           Because the change to the module is to address a security-relevant CVE, **the previous version of**  
1884           **the module is no longer considered validated and shall be removed from the certificate;**  
1885           exceptions may be made if the vendor shows how the CVE can be mitigated by policies included  
1886           in the Security Policy, while still adhering to the FIPS 140-3 standard.

1887           <sup>1</sup> A *security-relevant CVE* is one that affects how the module meets the security objectives and  
1888           requirements of the FIPS 140-3 standard.

#### 1889   7.1.12   Algorithm Transition (TRNS)

1890           A CSTL has been contracted to perform a revalidation for a module on which the vendor has  
1891           made FIPS 140-3 security relevant changes solely in response to a published CMVP algorithm  
1892           transition that will cause some previously validated modules to be placed on the Historical list  
1893           (see [Programmatic Transitions](#) webpage for a list of such algorithms). For example, the 2024  
1894           non-SP 800-56Brev2 RSA-based key encapsulation/un-encapsulation transition explained in  
1895           FIPS 140-3 [IG D.G](#). If the algorithm transition will NOT cause the module to move to the  
1896           historical list (i.e., considered a “soft” transition), changes cannot be made as part of this  
1897           submission.

1898           Note: a single Scenario TRNS submission may combine multiple algorithm transitions.  
1899           However, this may increase review time.

1900           The purpose of the TRNS revalidation is to provide the vendor a means to quickly address  
1901           algorithm transition requirements, test and revalidate a module in order to meet a CMVP  
1902           transition, while at the same time providing assurance that the module still meets the FIPS 140-3  
1903           standard.

1904           If the module code is *changed* to address an algorithm transition, the following requirements  
1905           apply:

- 1906           a. Submitted as a Scenario TRNS.

- 1907            b. The CSTL **shall** determine that security relevant changes to the module are only  
 1908            to address a specific CMVP transition. Other changes are permitted if only  
 1909            directly impacted by the TRNS change (e.g., addressing the TRNS may require  
 1910            changing the version number, and that requires the show version service be  
 1911            updated). In Web Cryptik, this may be captured as a checkbox under the TRNS  
 1912            submission scenario (e.g., the CSTL selects “Limited NSRL”).
- 1913            c. The CSTL **shall** examine each modification and confirm that the change does not  
 1914            conflict with the requirements of FIPS 140-3.
- 1915            d. The CSTL **shall** determine that no other modifications have been made. The  
 1916            vendor is not required to address IGs or guidance that have been published since  
 1917            submission of the original module, unless directly applicable to the transitioning  
 1918            algorithm (e.g., CAVP testing or self-test requirements).
- 1919            e. The CSTL **shall** identify the assertions affected by the security-relevant  
 1920            modification and **shall** perform the tests associated with those assertions.
- 1921            f. If the means to meet the transition are in the scope of an algorithm  
 1922            implementation, and the path chosen to meet the requirements necessitates testing,  
 1923            then this algorithm **shall** be CAVP tested to obtain a new CAVP certificate with  
 1924            the new module version. In Web Cryptik, this case is expected to be captured as a  
 1925            checkbox under the TRNS submission scenario (e.g., the CSTL selects “CAVP  
 1926            Testing Redone”).
- 1927            g. In addition to the tests performed against the affected assertions, the CSTL **shall**  
 1928            also perform the predefined regression tests shown on the [CMVP website](#) under  
 1929            “TRNS – Code Change” on all versions listed on the module’s certificate and on  
 1930            at least one of the listed OEs for hybrid or software/firmware modules (if the  
 1931            module binary image is identical across all OEs; if not, testing on at least every  
 1932            binary image is required).
- 1933            h. The CSTL **shall** provide justification on why regression testing is not necessary  
 1934            for the untested OEs. With proper justification, these may remain on the  
 1935            module’s certificate.
- 1936            i. If regression testing is not performed on some versions, then those **shall** be  
 1937            removed from the module’s certificate. OEs without proper justification or  
 1938            regression testing **shall** be removed from the module’s certificate.

1939            If the module code is *unchanged* to address an algorithm transition and the change is purely to  
 1940            documentation, one of the following four options apply. For each option, the CSTL **shall** state  
 1941            that the change to address the transition is purely documentary and which option applies.

1942            **Option 1:** services or functionality were not moved to or from an approved mode to remain  
 1943            compliant (e.g., previously non-compliant services remain in an approved mode but are updated  
 1944            to demonstrate compliance rather than moved into a non-approved mode), then the vendor may  
 1945            pursue a Scenario ALG revalidation.

- 1946 **Option 2:** The vendor moves all non-compliant functionality into a non-approved mode of  
 1947 operation from an approved mode of operation.
- 1948 a. Submitted as a Scenario TRNS.
- 1949 b. The CSTL **shall** determine that security relevant changes to the module are only  
 1950 to address a specific CMVP transition.
- 1951 c. The CSTL **shall** examine each modification and confirm that the change does not  
 1952 conflict with the requirements of FIPS 140-3.
- 1953 d. The CSTL **shall** determine that no other modifications have been made. The  
 1954 vendor is not required to address IGs or guidance that have been published since  
 1955 submission of the original module, unless directly applicable to the transitioning  
 1956 algorithm (e.g., CAVP testing or self-test requirements).
- 1957 e. The CSTL **shall** identify the assertions affected by the security-relevant  
 1958 documentation modification and **shall** perform the tests associated with those  
 1959 assertions.
- 1960 f. The CSTL **shall** demonstrate how the module still meets [IG 2.4.C](#) after the  
 1961 reclassification of non-compliant functionality into a non-approved mode of  
 1962 operation.
- 1963 g. In addition to the tests performed against the affected assertions, the CSTL **shall**  
 1964 also perform the predefined regression tests shown on the [CMVP website](#) under  
 1965 “TRNS - No Code Change” on all versions listed on the module’s certificate and  
 1966 on at least one of the listed OEs for hybrid or software/firmware modules (if the  
 1967 module binary image is identical across all OEs; if not, testing on at least every  
 1968 binary image is required).
- 1969 The only exception to this requirement (g.) is if the algorithm being transitioned is  
 1970 part of a standalone service and is not used by any other module service (e.g.,  
 1971 cryptographic library where the module only provides the algorithm as an API  
 1972 service to a calling application as a stand-alone service). In this case, the CSTL  
 1973 **shall** provide justification on why regression testing is not necessary at all.
- 1974 j. The CSTL **shall** provide justification on why regression testing is not necessary  
 1975 for the untested OEs. With proper justification, these may remain on the  
 1976 module’s certificate.
- 1977 k. If regression testing is not performed on some versions, then those **shall** be  
 1978 removed from the module’s certificate. OEs without proper justification or  
 1979 regression testing **shall** be removed from the module’s certificate.
- 1980 h. The CSTL **shall** provide assurance that the non-compliant functionality is not  
 1981 used to meet any FIPS 140-3 requirements (key/CSP establishment, generation,  
 1982 storage, etc.).
- 1983 i. The CSTL **shall** provide assurance, upon module examination, that no service,  
 1984 algorithm or CSP that relied on or used the non-compliant functionality,

1985 parameters, keys, etc. remain in an approved mode. An approved mode **shall**  
 1986 only contain approved services.

1987 j. Documentation **shall** be updated to indicate the module does not utilize non-  
 1988 compliant functionality in an approved mode of operation.

1989 **Option 3:** The vendor recategorizes the non-compliant functionality as claiming no security per  
 1990 [IG 2.4.A](#), and this functionality remains in an approved mode of operation.

- 1991 a. The same rules for Option 2 above **shall** be followed except for bullets ‘i’ and ‘j’.  
 1992 b. The CSTL **shall** provide justification on how the requirements of [IG 2.4.A](#) are  
 1993 met. This scenario is intended to be rarely used/accepted and depends on the  
 1994 purpose or use of the service that utilizes the non-approved algorithms. For  
 1995 example, a software library implementing three-key Triple-DES Encryption as  
 1996 one of its approved services cannot simply state this algorithm does not claim any  
 1997 security (per [IG 2.4.A](#)) and be used in an approved mode, as this does not meet 3)  
 1998 or 4) in [IG 2.4.A](#) Additional Comment #2.

1999 **Option 4:** A combination of any of three options above (CAVP testing, moving non-compliant  
 2000 functionality into the a non-approved mode, and/or recategorized per [IG 2.4.A](#)), in which case,  
 2001 requirements of each option apply.

- 2002 a. Submitted as a Scenario TRNS.  
 2003 b. Each option **shall** be listed/indicated in the Revalidation Change Document under  
 2004 Option 4 (e.g. under Option 4, the following are claimed: Options 1 and 2) and  
 2005 note how each of the applicable ‘shall’ statements for each option are met).

2006 In order to accommodate vendors who are updating their validation to prepare for an algorithm  
 2007 transition, fully compliant TRNS or ALG revalidations that have addressed the transition and are  
 2008 submitted to the CMVP before the date the transition is to take effect, will remain on the active  
 2009 list through the completion of the revalidation, even if it is not completed until after the transition  
 2010 date, unless the algorithm transition is to address a security concern that is deemed unacceptable  
 2011 by the CMVP. For newly submitted ALG submissions that address the transition, the CSTL  
 2012 **shall** include in the Special Instructions field the text “algorithm\_transition” (with or without the  
 2013 underscore) in order for the CMVP not to move this submission to the historical list come the  
 2014 algorithm transition date.

2015 Changes made to a module, whether to the module code or purely to documentation, in order to  
 2016 meet a transition are security-relevant, due to their potential impacts on core and downstream  
 2017 services and the treatment of keys and SSPs. For example, moving *allowed* functionality from  
 2018 an approved mode to a non-approved mode - by either changing the software/firmware or a  
 2019 purely documentation change - is considered security relevant. Therefore, besides the case in  
 2020 **Option 1** above, all submissions that address a transition will require a Scenario UPDT, TRNS  
 2021 or FS submission regardless of module type or security level.

2022 If a Scenario TRNS revalidation addresses an algorithm transition that moved the original  
 2023 certificate to the Historical list, and the sunset date of the certificate has yet to expire, then upon  
 2024 the revalidation of the module under Scenario TRNS, a new certificate will be issued on the  
 2025 Active list (inheriting the original sunset date) for the version of the module compliant with the

2026 transition requirements. Otherwise, if the original certificate was moved to the Historical list for  
2027 reasons that are not addressed in the TRNS revalidation (e.g., a separate algorithm transition or  
2028 the sunset date expired), the new certificate will be shown on the Historical list *immediately* after  
2029 completion of the TRNS revalidation.

#### 2030 7.1.13 Physical Enclosure (PHYS)

2031 Modifications are made only **to the physical enclosure of the cryptographic module that**  
2032 **provides its protection and involves no operational changes to the module.** The CSTL is  
2033 responsible for ensuring that the change only affects the physical enclosure (integrity) and has no  
2034 operational impact on the module. The CSTL **shall** fully test the physical security features of the  
2035 new enclosure to ensure its compliance to the applicable requirements of the standard.

2036 The CSTL **shall**:

- 2037 a. Describe the change (pictures may be required),
- 2038 b. State that it is a security relevant change,
- 2039 c. Provide sufficient information supporting that the physical only change has no  
2040 operational impact,
- 2041 d. Describe the tests performed by the CSTL that confirm that the modified enclosure still  
2042 provides the same physical protection attributes as the previously validated module. For  
2043 physical security levels 2, 3 and 4, the CSTL **shall** submit an updated Physical Security  
2044 Test Report.

2045 7.1.14 Submission Scenario Summary Table

Scenario	<u>A</u> ctive or <u>H</u> istorical <sup>1</sup>	New or Updated Cert <sup>2</sup>	New Sunset Date <sup>3</sup>	Meet All Latest Guidance <sup>4</sup>	Entropy Testing Applicable (ESV) <sup>5</sup>	ENT Remain on Cert <sup>7</sup>	Predefined Regression Testing <sup>8</sup>	Submission Process <sup>9</sup>
VUP	A or H	Updated	No	No	No	Possible	No (nor optional testing)	Email
VAOE	A or H	Updated	No	No	No	Possible	No (nor optional testing)	Email
NSRL	A only	Updated	No	No	No	Possible	No	Email
ALG	A only	Updated	No	No (except for the updated algorithm)	No	Possible	No	Email
OEUP	A only	Updated	No	No	Yes <sup>6</sup>	Possible	Yes (full regression table)	Email
RBND	A only	New	No	No	No	Possible	No (nor optional testing)	Email
PTSC	A only	New	No	No	Yes <sup>6</sup>	Possible	Yes (full regression table)	Email
UPDT	A or H	New	Yes	Yes	Yes	No	Yes (full regression table)	Web Cryptik
CVE	A or H	Updated	No	No	No	Possible	Yes (subset of regression table)	Email
TRNS	A or H	New	No	No (except for the algorithm transitioning)	No	Possible	Yes (subset of regression table)	Email
PHYS	A only	Updated	No	No	No	Possible	Yes (physical security)	Email
FS	N/A	New	Yes	Yes	Yes	No	Full testing	Web Cryptik

2046 <sup>1</sup> A or H means the revalidation can be on a completed validation that is either Active *or* Historical; A  
 2047 only means it can only be on an Active validation.

2048 <sup>2</sup> The result of this validation or revalidation will either be a new certificate (new number) or an updated  
 2049 certificate (same number).

2050 <sup>3</sup> The result of this validation or revalidation will either be a new sunset date of 5 years, or the sunset date  
 2051 will remain the same. See Additional Comment #3 below for more details.

2052 <sup>4</sup> If Yes, the validation or revalidation **shall** meet all the latest applicable guidance and requirements (e.g.,

2053 standards, implementation guidance, management manual guidance, algorithm testing/self-tests, and other  
 2054 CMVP guidance) at the time of submission to the CMVP unless there is an implementation guidance  
 2055 transition that affects reports in the queue. If No, the revalidation **shall** meet all applicable requirements  
 2056 at the time of *original* validation (a module does not need to meet requirements that were added since the  
 2057 time of original validation, except those specified in the table).

2058 <sup>5</sup> If applicable per [IG 9.3.A](#).

2059 <sup>6</sup> Only required on the new OEs for OEUP, or new single-chip environments for PTSC.

2060 <sup>7</sup> Only for the original validation's ENT claim. No new ENT claims are possible, for any validation or  
 2061 revalidation.

2062 <sup>8</sup> Note: additional regression testing (on top of the predefined ones) may be applicable per requirements of  
 2063 the scenario. See the [CMVP FIPS 140-3 Resources](#) page for the pre-defined regression tests.

2064 <sup>9</sup> The CMVP has emailed the CSTLs with additional revalidation scenario guidance that details the  
 2065 temporary submission processes as these scenarios are being incorporated into Web Cryptik.

#### 2066 7.1.15 Additional Comments

- 2067 1. If the individual section(s) security level is being lowered as part of the revalidation,  
 2068 this is considered security relevant and the module may be submitted as a UPDT with  
 2069 full testing on the individual section(s) that is being lowered or impacted by the  
 2070 change.
- 2071 2. If the individual section(s) security level is being raised or if the physical embodiment  
 2072 changes, e.g., from multi-chip standalone to multi-chip embedded, then the  
 2073 cryptographic module will be considered a new module and **shall** undergo full  
 2074 validation testing by a CSTL and submitted as an FS.
- 2075 3. The sunset date for the module is determined based on the scenario:
  - 2076 • Scenarios FS, UPDT – sunset date will be 2 years (interim validation) or 5 years  
 2077 (full validation) from the validation date
  - 2078 • Scenarios VUP, VAOE, NSRL, ALG, OEUP, CVE, PHYS – sunset date unchanged
  - 2079 • Scenarios RBND, PTSC, TRNS – sunset date is inherited from the original  
 2080 certificate
- 2081 4. It is **not** possible to combine any revalidation scenarios outside of what is explicitly  
 2082 permitted by the submission scenario. For example, if a vendor would like to rebrand  
 2083 (RBND) a PTSC submission, this would need to happen in two separate submissions (i.e.,  
 2084 RBND followed by a PTSC). Similarly, despite it being a simple change, a VUP or VAOE  
 2085 would need to be submitted separately to address any vendor admin change or vendor  
 2086 affirmed OE changes, respectfully, and cannot be combined with other scenarios. This will  
 2087 give the CMVP the most flexibility to address each scenario submission effectively and  
 2088 efficiently.

2089

2090 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	-	-	✓	x	-	-	-	-	-	-	-
	RBND	x	-	✓	✓	-	-	-	-	-	-	✓
	PTSC	-	-	✓	✓	-	-	-	-	-	-	-
	UPDT	-	-	x	✓	✓	✓	✓	-	✓	✓	✓
	CVE	-	-	✓	✓	-	-	-	-	-	-	-
	TRNS	-	-	✓	✓	-	-	-	-	-	-	-
	PHYS	-	-	-	-	-	-	-	-	-	-	-

2091 x - The Added/secondary scenario will NOT be separately selectable as a sub-option in  
 2092 WebCryptik (e.g., VUP changes will always be possible under a RBND).  
 2093 ✓ - The Added/secondary scenario WILL be separately selectable as a sub-option. The  
 2094 Added/secondary scenario may be further locked down / limited per the Main Submission  
 2095 definition (e.g., NSRL changes associated with an OEUP submission must be specific to running  
 2096 the new OEs, rather than permitting *any* NSRL changes).  
 2097

2098 For the revalidation scenarios that *can* be combined (i.e., checkbox in the table above), the  
 2099 main submission **shall** meet all applicable requirements of the added/secondary scenario, in  
 2100 addition to the main scenario requirements. For example, a RBND + NSRL must include  
 2101 proper regression testing and documenting the changes per NSRL specifications.

2102 5. A revalidation submission cannot be performed on a submission that is in the queue. It  
 2103 **shall** be on a completed validation (e.g., UPDT on a *validated* FS). However, see sections  
 2104 4.4.5 (*Resubmission while in Review Pending*) and 4.4.6 (*Changes while in Coordination*)  
 2105 for permitted changes while in the queue within the same submission.

2106 **7.2 CMVP requirements pertaining to testing and approved algorithms**

2107 FIPS 140-3 describes approved security functions which can be used in an approved mode of  
 2108 operation, and non-approved security functions which cannot be used in an approved mode of  
 2109 operation. Approved security functions are expected to be CAVP tested, but CAVP testing has  
 2110 not always been available for these methods.

2111 In such cases where CAVP testing is not available, guidance must be written to permit using  
 2112 these algorithms in an approved mode. These algorithms may be “vendor affirmed” to meet the  
 2113 applicable standard(s).

2114 In addition, security methods that fall outside of the list of approved methods cannot be used in  
 2115 an approved mode, unless guidance is written to permit such special cases, where these methods  
 2116 are *allowed* to be used in the approved mode of operation; or as permitted under AS02.21.

2117 This section explains when vendor affirmed or *allowed* methods are permitted, as well as the  
 2118 transitioning from vendor affirmed to CAVP Testing.

### 2119 7.2.1 Vendor Affirmation of Security Functions and Methods

2120 If CAVP testing is not available or the module is submitted during a transition period, then the  
 2121 following guidance is applicable.

2122 If new approved methods (e.g., NIST FIPS, SP, etc.) are added to SP 800-140 documents, until  
 2123 such time that CAVP testing is available or the transition period has not yet expired for the new  
 2124 method, the CMVP will:

- 2125 ○ if applicable, allow methods as provided by existing guidance (untested, and listed as  
 2126 non-approved but *allowed* in an approved mode as shown in IGs [D.F](#) and [D.G](#)); and
- 2127 ○ permit the vendor to implement the new approved method if an IG that supports  
 2128 vendor affirmation of this algorithm is published and met (untested, listed as  
 2129 approved for use in an approved mode with the caveat “vendor affirmed”).

2130 Note:

- 2131 1. The Cryptographic Technology Group (CTG) at NIST may determine prior methods may be  
 2132 retroactively disallowed and moved to non-approved and not permitted in an approved mode  
 2133 of operation (e.g., DES). A transition notice would appear in NIST publications.
- 2134 2. For all approved methods, all applicable FIPS 140-3 requirements **shall** be met. An IG may  
 2135 further clarify the requirements for a vendor affirmed algorithm.

### 2136 Additional Comments

2137 **Vendor Affirmed:** a security method reference that is listed with this caveat has not been tested  
 2138 by the CAVP, and the CMVP or CAVP provide no assurance regarding its correct  
 2139 implementation or operation. Only the vendor of the module affirms that the method or  
 2140 algorithm was implemented correctly.

2141 The users of cryptographic modules implementing vendor affirmed security functions must  
 2142 consider the risks associated with the use of untested and unvalidated security functions.

### 2143 7.2.2 Transitioning from vendor affirmed to CAVP Testing

2144 When CAVP algorithm testing is released on the ACVTS production server in any of the  
 2145 following 3-month periods identified below, the transition occurs at the end of the following 3-  
 2146 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

2147 *Table 1 - CAVP testing release dates and subsequent CMVP Transition dates*

2148 To illustrate, if the CAVP releases new testing for algorithm A, B and C, during the July 1 –  
 2149 September 30 period, then the transition date will be September 30 + three months, so after  
 2150 December 31 vendor affirming to algorithms A, B, or C will be prohibited in initial report  
 2151 submissions.

2152 During the transition period, a new approved method would either be listed as approved with a  
 2153 reference to a CAVP validation certificate, or as vendor affirmed if testing was not performed  
 2154 and an IG that supports vendor affirmation of this algorithm was met.

2155 When the transition period ends, for newly received test reports:

- 2156 ○ only approved methods that have been tested, receives a CAVP validation certificate  
 2157 and is verified to meet the underlying algorithm standard is permitted. All other  
 2158 methods would be listed as non-approved and not allowed in an approved mode of  
 2159 operation.
- 2160 ○ the vendor could optionally follow up with testing of untested vendor affirmed methods  
 2161 and if so, the reference to vendor affirmed would be removed and replaced by reference  
 2162 to the algorithm certificate. If there are no changes to the module, this change can be  
 2163 submitted under Scenario ALG (see Section 7.1 – *Submission Scenarios*). If the  
 2164 module is changed, this can be submitted under Scenarios UPDT or FS as applicable.

2165 **Note:** To track the algorithms and their transition dates, the CMVP maintains a table available on  
 2166 ([https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions)  
 2167 [transitions](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/programmatic-transitions) ).

2168 **Note:** If a self-test requirement is associated with the algorithm, the algorithm will only be  
 2169 considered as an approved algorithm by CMVP if the self-test requirement is also met.

### 2170 7.3 Testing using Emulators and Simulators

2171 Under certain circumstances it may not be possible to test a module or algorithm directly. In  
 2172 these cases, CMVP has permitted the use of emulators and simulators to model the behavior of

2173 the item being tested. It is important to note the differences of these models and to apply them  
2174 under the correct circumstances.

2175 An emulator attempts to “model” or “mimic” the behavior of a cryptographic module. The  
2176 correctness of the emulators' behavior is dependent on the inputs to the emulator and how the  
2177 emulator was designed. It is not guaranteed that the actual behavior of the cryptographic module  
2178 is identical, as other variables may not be modeled correctly or with certainty.

2179 A simulator exercises the actual source code (e.g., Very High-Speed Integrated Circuit (VHSIC)  
2180 Hardware Description Language (VHDL) code) prior to physical entry into the module (e.g., a  
2181 Field-Programmable Gate Array (FPGA) or custom Application-Specific Integrated Circuit  
2182 (ASIC)). From a behavioral perspective, the behavior of the source code within the simulator  
2183 may be logically identical when placed into the module or instantiated into logic gates. However,  
2184 many other variables exist that may alter the actual behavior (e.g., path delays, transformation  
2185 errors, noise, environmental, etc.). It is not guaranteed that the actual behavior of the  
2186 cryptographic module is identical, as many other variables may not be identified with certainty.

2187 Labs may apply emulators or simulators depending on the type of testing results to be achieved.  
2188 There are three broad areas of focus during the testing of a cryptographic module: operational  
2189 testing of the module at the defined boundary of the module, algorithm testing and operational  
2190 fault induction testing.

- 2191 1. Operational Testing – Emulation or simulation is prohibited for the operational testing of a  
2192 cryptographic module. Actual testing of the cryptographic module must be performed  
2193 utilizing the defined ports and interfaces and services that a module provides. A test  
2194 harness or a modified version to induce an error may be utilized; however, no changes to  
2195 code or circuitry responsible for the tested response may be made.
- 2196 2. Operational Fault Induction – An emulator or simulator may be utilized for fault induction  
2197 to test a cryptographic module’s transition to error states as a complement to the source  
2198 code review. Rationale must be provided for the applicable TE as to why a method does  
2199 not exist to induce the actual module into the error state for testing.
- 2200 3. Algorithm Testing – Algorithm testing utilizing the defined ports and interfaces and  
2201 services that a module provides is the preferred method. This method most clearly meets  
2202 the requirements of [IG 2.3.A](#). If this preferred method is not possible where the module’s  
2203 defined set of ports and interfaces and services do not allow access to internal algorithmic  
2204 engines, two alternative methods may be utilized:
  - 2205 a. A module may be modified under the supervision of the CSTL for testing purposes  
2206 to allow access to the algorithmic engines (e.g., test jig, test API), or
  - 2207 b. A module simulator may be utilized.

2208 When submitting the algorithm test results to the CAVP, the actual OE on which the  
2209 testing was performed must be specified (e.g., including modified module identification or  
2210 simulation environment). When submitting the module test report to the CMVP, AS2.20  
2211 must include rationale explaining why the algorithm testing was not conducted on the  
2212 actual cryptographic module. An emulator may not be used for algorithm testing.

## 2213 7.4 Remote Testing of Modules

2214 The guidance below addresses the need for testing a module remotely while obtaining the  
 2215 equivalent assurance as if the test were performed at the **vendor's facility**. All physical security  
 2216 testing except for Environment failure protection/testing (i.e., EFT/EPT tests: TE.07.73.01,  
 2217 TE.07.77.01-03 and TE.07.81.01-02) **shall** be performed in person by a CSTL tester at either the  
 2218 vendor, the CSTL site and/or remote site as per HB 150-17 requirements.

2219 The CSTL may perform some or all testing remotely. If the testing is performed remotely at the  
 2220 vendor site, the following conditions **shall** be met:

- 2221 1. a. The hardware, firmware or hybrid IUT is located at the vendor site.
- 2222 b. The software IUT is located at the vendor site or 3<sup>rd</sup> party cloud system.
- 2223 2. The vendor remotely provides a cryptographic module to the test laboratory and its  
 2224 boundary and version are verified against the Security Policy. (ISO/IEC 24759  
 2225 TE04.13.01, 02, 03). The module boundary and version **shall** be verified at the beginning  
 2226 of any new remote testing sessions.
- 2227 3. a. The network access and/or video conference to a remote test operational environment,  
 2228 in support of actual testing, **shall** be authorized and controlled by the vendor.
- 2229 b. A 3<sup>rd</sup> party cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google  
 2230 Cloud) may be used as a service in support of module validation (e.g. video conference  
 2231 and data storage) if:
  - 2232 • all HB 150-17 and NVLAP General Criteria Checklist ISO\_IEC 17025  
 2233 requirements are met; and
  - 2234 • the remote testing requirements are met.
- 2235 c. A cloud system (e.g., Amazon Web Services, Microsoft Azure, and Google Cloud)  
 2236 may be used as a testing platform if:
  - 2237 • all HB 150-17 and NVLAP General Criteria Checklist ISO\_IEC 17025  
 2238 requirements are met;
  - 2239 • the remote testing requirements are met;
  - 2240 • the environment provides the same level or additional level of security as  
 2241 the lab would provide for internal testing;
  - 2242 • the cryptographic module under test **shall** be confirmed to be running on  
 2243 an OE that is well-defined and has a specific OS version, hardware  
 2244 platform and version, and processor (including microprocessor version) as  
 2245 shown on the module's certificate and security policy; and
  - 2246 • the OS version, hardware platform and version, and processor **shall** be  
 2247 confirmed during the testing session.

- 2248 d. As permitted within a signed agreement by the lab and vendor:
- 2249                   • The tester’s network **shall** be connected to the vendor’s network via a
- 2250                   secure connection (e.g., VPN or SSH) ; and/or
- 2251                   • A secure video conference **shall** be used and the recording done in a
- 2252                   secure manner.
- 2253
- 2254 e. The tester’s tools must satisfy the lab’s network requirements before connecting to the
- 2255                   vendor’s network to test the module if applicable.
- 2256 4. The CSTL **shall** have a procedure for conducting remote testing at the vendor site which
- 2257                   includes the following:
- 2258                   a. All the remote testing sessions that produce the final test results **shall** be recorded and
- 2259                   archived at the CSTL as evidence material to demonstrate the tester control and/or
- 2260                   oversight (as per bullet 6 below) (e.g. video conference records and/or detailed test plan)
- 2261                   and to capture the test results (e.g. video conference records, screenshots and/or log files).
- 2262                   b. If multiple remote testing sessions are required, a log which includes the date and the
- 2263                   test being conducted **shall** be maintained and archived.
- 2264                   c. If during testing, the IUT version or subversion (e.g. pre-release, debug) changes, the
- 2265                   final test report being submitted **shall** reflect the final version of the IUT.
- 2266                   d. If there are multiple simultaneous testing activities occurring at the vendor site, a
- 2267                   system of separation between the different cryptographic module test activities **shall** be
- 2268                   maintained.
- 2269                   e. For all conformance testing and validations, the CSTL **shall** ensure that any file
- 2270                   containing iterative, not final, test results are isolated from the final test results.
- 2271                   f. It is the CSTL’s responsibility to ensure that any version iteration during the testing
- 2272                   doesn’t impact any of the final results transmitted to the CMVP.
- 2273 5. The required operational environment information (e.g., operating system name and
- 2274                   version, processor family, hardware platform model) **shall** be obtained and verified
- 2275                   against the operational environment information listed on the CAVP algorithm certificates
- 2276                   for this module.
- 2277 6. The tester is accountable and therefore **shall** understand, oversee, direct, and/or assume
- 2278                   control of testing operations to initialize, install, and operate the module. The tester is
- 2279                   accountable to ensure the proper initialization, installation and operation of the module
- 2280                   through the entire testing at the CSTL site and/or vendor site for the multiple testing
- 2281                   sessions as applicable.
- 2282 7. If a test harness is used, it **shall** be reviewed or written by the lab. It **shall** be verified to
- 2283                   have been maintained properly with no vendor manipulation prior to its execution. The
- 2284                   test results on the remote operational environment **shall** be captured and transmitted back

2285 to lab without the risk of being modified. The tester **shall** verify the test harness runs  
 2286 properly on its operational environment. The tester must verify the integrity of the testing  
 2287 session as well as the completeness and accuracy of the test results.

2288 8. The remote testing **shall** cover the same set of FIPS 140-3 requirements including but not  
 2289 limited to the following list, as if the operational environment were local to the tester:

2290 a. The services listed in the module Security Policy can be invoked or directed/overseen  
 2291 and verified by the tester.

2292 b. For a module to be validated at Level 2 or 3 for ISO/IEC 19790:2012 Section 7.4.4,  
 2293 the role-based or identity-based authentication **shall** be performed or  
 2294 directed/overseen and verified by the tester.

2295 c. The failure of self-tests and the subsequent transition to an error state where module  
 2296 data output interfaces are inhibited can be observed and verified by the tester.

2297 d. As applicable per IG 9.3.A, entropy has been effectively analyzed and received an  
 2298 ESV for all specific OEs and/or platforms prior to submission.

2299 The vendor must provide a signed affirmation letter to the lab describing the remote testing  
 2300 process and access control mechanism that allows the lab to perform the test on the remote  
 2301 operational environment and protects the integrity of the test results. The lab **shall** provide a  
 2302 signed letter to the CMVP stating that the module had been tested remotely, affirming that the  
 2303 vendor provided their affirmation letter, stating what TEs were tested remotely, and explaining  
 2304 how the requirements were met during the remote testing.

2305 It is the CSTL's responsibility to ensure that the assurance level is maintained when remote  
 2306 testing is being conducted.

2307 Additional Comments:

2308 1. It is the responsibility of the tester to determine if a module is eligible to be tested remotely. If  
 2309 the tester cannot demonstrate a test requirement during remote testing, then the module **shall** not  
 2310 be fully tested remotely. If the tester wishes to test a subset of test requirements remotely, the  
 2311 remaining test requirements **shall** be tested onsite at the CSTL site or in person by the CVP tester  
 2312 at the vendor site.

2313 2. The tester **shall** confirm that the operational environment exactly matches the agreed upon test  
 2314 environment, including any virtual environments used. A Virtual Machine may not be used in  
 2315 lieu of an OS, unless the VM has been agreed to be part of the test environment and will be listed  
 2316 on the certificate.

2317 3. A record of the testing location, related documentation (e.g. equipment proof of calibration)  
 2318 and CSTL tester(s) who conducted the testing **shall** be maintained. This is applicable for all  
 2319 tests including physical security testing.

2320 4. The above vendor site remote testing requirements are also applicable to 3<sup>rd</sup> party remote site  
 2321 in addition to existing the HB 150-17 and NVLAP General Criteria Checklist ISO\_IEC 17025  
 2322 requirements.

2323 5. Regardless of the location of the testing, it is the CSTL’s responsibility to ensure that all HB  
 2324 150-17 and NVLAP General Criteria Checklist ISO\_IEC 17025 requirements are met (e.g.  
 2325 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,  
 2326 7.1.4, B.2.2 & B.3 requirements).

2327 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>.  
 2328

## 2329 7.5 Partial validations and non-applicable areas

2330 CMVP will not issue a validation certificate unless the cryptographic module meets at least the  
 2331 Security Level 1 requirements for each area in Section 6 of ISO/IEC 24759:2017. Areas can be  
 2332 designated as Not Applicable (N/A) if they meet the following criteria:

- 2333 • Section 6.5, Software/Firmware Security may be designated as N/A if the module is  
 2334 hardware-only without firmware or software;
- 2335 • Section 6.6, Operational Environment may be designated as N/A if the operational  
 2336 environment for the cryptographic module is a limited or non-modifiable operational  
 2337 environment and Section 6.7, Physical Security is greater than Security Level 1  
 2338 (AS06.04).
- 2339 • Section 6.7, Physical Security may be designated as N/A if the cryptographic module is a  
 2340 software-only module and thus has no physical protection mechanisms;
- 2341 • Section 6.8, Non-invasive security is N/A as there are currently no requirements in SP  
 2342 800-140F. Any claims for non-invasive will be identified under Section 6.12.
- 2343 • Section 6.12, Mitigation of Other Attacks is Applicable if the module has been purposely  
 2344 designed, built, and publicly documented to mitigate one or more specific attacks.  
 2345 Otherwise, this section may be designated as N/A.

## 2346 7.6 CMVP requirements for PIV validations

2347 PIV card applications can only be tested on a CMVP validated module, such as a smartcard. The  
 2348 CMVP validated module then obtains NPIVP validation, by adding the PIV card application to  
 2349 the module. The validated smartcard and the PIV card application is then re-validated as a  
 2350 CMVP module.

2351 A PIV card application that is included as a component of a cryptographic module **shall** be  
 2352 referenced on the module validation. The cryptographic module validation entry **shall** provide  
 2353 reference to the PIV card application(s) validation certificate number. The cryptographic  
 2354 module’s versioning information **shall** include the complete versioning information of the  
 2355 module including the PIV application(s). Each PIV application’s name **shall** be clearly  
 2356 identified, and the PIV Certificate number is referenced on the CMVP module validation.

2357 The PIV NPIVP validation entry includes the following information:

- 2358 1. the name of the PIV card application,

- 2359        2. the name of the cryptographic module the PIV application was tested on, and  
 2360        3. the complete versioning information of the module including the PIV application(s)

2361 The NPIVP validation entries can be found at:

2362 [http://csrc.nist.gov/groups/SNS/piv/npivp/validation\\_lists/PIVCardApplicationValidationList.ht](http://csrc.nist.gov/groups/SNS/piv/npivp/validation_lists/PIVCardApplicationValidationList.htm)  
 2363 [m](http://csrc.nist.gov/groups/SNS/piv/npivp/validation_lists/PIVCardApplicationValidationList.htm)

## 2364 **7.7 Module count definition**

2365 Moved to the following CMVP webpage, under “MIS Field Descriptions”:

2366 <https://csrc.nist.gov/projects/cmvp/sp800-140b>

## 2367 **7.8 Module definitions for same certificates**

2368 To be on the same certificate, each module version **shall** have identical:

- 2369        1. Section and overall levels.  
 2370        2. Suite of approved security services.  
 2371        3. Cryptography.  
 2372        4. Suite of security functions and underlying algorithms, modes, and key sizes.  
 2373        5. Suite of SSPs associated with the security services.  
 2374        6. Suite of roles and authentication methods.  
 2375        7. Finite State Model except related to the allowed differences.  
 2376        8. SSP establishment methods.  
 2377        9. Self-tests.  
 2378        10. Design assurance.  
 2379        11. Mitigation of other attacks.  
 2380        12. Module type (i.e., Software, Hardware, Firmware, or Hybrid).  
 2381        13. Module embodiments (i.e., single-chip, multi-chip embedded/standalone) with similar  
 2382        physical construction including physical boundary.

## 2383 **7.9 Vendor or User Affirmation of Modules**

2384 The tested/validated module version, OE upon which it was tested, and the originating vendor  
 2385 are stated on the validation certificate entry. The certificate validation entry serves as the  
 2386 benchmark for the module-compliant configuration. This guidance addresses two separate  
 2387 scenarios: changes a **Vendor** (7.9.1) can affirm the module will perform as tested in the CSTL’s  
 2388 validation submission and changes a **User** (7.9.2) can affirm the module will perform as tested in  
 2389 the CSTL’s validation submission.

2390 This guidance is *not applicable* for validated modules when the requirements of **ISO/IEC**  
 2391 **19790:2012** Section 7.7 Physical Security has been validated at Levels 2 or higher. This  
 2392 guidance is however, applicable at Level 1 for *firmware* or *hybrid* modules.

## 2393 7.9.1 Vendor

2394 1. A vendor may perform post-validation recompilations of a software or firmware module and  
 2395 affirm the modules continued validation compliance. By adding vendor support of non-tested  
 2396 configurations to the validated module security policy, the vendor bears all responsibility.  
 2397 These non-tested configurations versions may be considered by the user at their risk,  
 2398 provided the following is maintained:

2399 a) Software modules that do not require any source code modifications (e.g., changes,  
 2400 additions, or deletions of code) to be recompiled and ported to another OE must:

2401 i) For **Level 1 OE**, a software cryptographic module can be considered compliant with  
 2402 the FIPS 140-3 validation when operating on any general-purpose platform/processor  
 2403 that supports the specified operating system as listed on the validation entry or  
 2404 another compatible<sup>5</sup> operating system, or

2405 ii) For **Level 2 OE**, a software cryptographic module can be considered compliant with  
 2406 the FIPS 140-3 validation when operating on any general-purpose platform/processor  
 2407 that supports the same level 2 operational environment settings specified on the  
 2408 validation entry.

2409 b) Firmware modules that do not require any source code modifications (e.g., changes,  
 2410 additions, or deletions of code) to be recompiled, and its identified unchanged tested  
 2411 operating system (i.e., same version or revision number) may be ported together from one  
 2412 platform to another platform while maintaining the module's validation.

2413 Level 2 and above Firmware modules cannot be ported and maintain their validation,  
 2414 since Physical Security must be retested.

2415 c) Hybrid modules may be ported together from one OE to another OE while maintaining  
 2416 the module's validation provided that they do not require any of the following:

2417 i) software or firmware source code modifications (e.g., changes, additions, or deletions  
 2418 of code) to be recompiled and its identified unchanged tested operating system (i.e.,  
 2419 same version or revision number) or another compatible operating system;

2420 ii) modified hardware components utilized by the software or firmware (e.g., changes,  
 2421 additions, or deletions).

2422 Level 2 and above hybrid modules cannot be ported and maintain their validation, since  
 2423 Physical Security must be retested.

2424 The CMVP allows vendor porting and re-compilation of a validated software, firmware or  
 2425 hybrid cryptographic module from the OE specified on the validation certificate to an OE  
 2426 which was not included as part of the validation testing as long as the porting rules are  
 2427 followed. Vendors may affirm that the module works correctly in the new OE. However, the  
 2428 CMVP makes no statement as to the correct operation of the module or the security strengths

---

<sup>5</sup> 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.

2429 of the generated keys when so ported if the specific OE is not listed on the validation  
2430 certificate.

2431 The vendor **shall** work with a CSTL to update the security policy and submit it to the CMVP  
2432 under one of the available revalidation scenarios (see Scenario VAOE in Section 7.1). The  
2433 update would affirm and include references to the new vendor affirmed OE(s) (see related  
2434 table in SP 800-140B and SP 800-140Brev1). The module's Security Policy **shall** include a  
2435 statement that no claim can be made as to the correct operation of the module or the security  
2436 strengths of the generated keys when ported to an OE which is not listed on the validation  
2437 certificate.

2438 2. Software or firmware modules that require source code modifications (e.g., changes,  
2439 additions, or deletions of code) to be recompiled and ported to another hardware or OE must  
2440 be reviewed by a CSTL and revalidated per [Section 7.1](#) (including regression testing) to  
2441 ensure that the module does not contain any OE-specific or hardware environment-specific  
2442 code dependencies. See Scenarios UPDT, NSRL, and OEUP. This is not porting but rather  
2443 incorporating the new versions and environment onto the certificate.  
2444

2445 The vendor must meet all applicable requirements in ISO/IEC 19790:2012 Section 7.11, SP 800-  
2446 140 Section 6.11, and CMVP IGs.

## 2447 7.9.2 User

2448 **A user may not modify a validated module. Any user modifications invalidate a module**  
2449 **validation.**<sup>6</sup>

2450 A user may perform post-validation porting of a module and affirm the module's continued  
2451 validation compliance provided the following is maintained:

2452 1. For **Level 1 OE**, a software, firmware, or hybrid cryptographic module will remain  
2453 compliant with the FIPS 140-3 validation on any general-purpose platform/processor that  
2454 supports the specified operating system listed on the validation entry, or another compatible  
2455 operating system.

2456 The user may affirm that the module works correctly in the new OE if the porting rules are  
2457 followed. However, the CMVP makes no statement as to the correct operation of the module or  
2458 the security strengths of the generated keys when ported and executed in an OE not listed on the  
2459 validation certificate.

## 2460 7.10 Operational Equivalency Testing for HW Modules

2461 CMVP requires full testing of any module that the vendor wishes to list on the certificate.  
2462 However, modules may be grouped together if they are the same except for devices listed under  
2463 Equivalence Categories, which are currently considered for five classes of devices. Each

---

<sup>6</sup> 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.

2464 Category and sample technologies for each Category are provided in Table 2.

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

2465 *Table 2 - Equivalence Categories*

2466 For details on the Equivalency Categories, please see the Equivalency Categories Tables under  
 2467 the [FIPS 140-3 Resources Tab](#) of the CMVP website. Also note, for modules that have  
 2468 differences within each of those categories, the level of testing required is dependent on the  
 2469 differences. Some differences require analysis only, while others require full or limited  
 2470 regression testing. The following are the general categories of the levels of testing. The actual  
 2471 testing required depends on the Equivalency Category (See Equivalency Regression Test Table  
 2472 and Equivalency Categories Tables found under the [FIPS 140-3 Resources Tab](#) of the CMVP  
 2473 website):

- 2474 - Analysis Only (AO) for Equivalency Category X: Once the equivalency evidence/argument  
 2475 is provided and validated for the Equivalency Category X, there is no additional test other  
 2476 than the proof of its physical existence required on a module with the equivalent components  
 2477 in Category X to the module that has been fully tested under the same validation.
- 2478 - Required Testing (RT) for Equivalency Category X:  
 2479
  - If a module has some security relevant differences in the Equivalency Category X, the

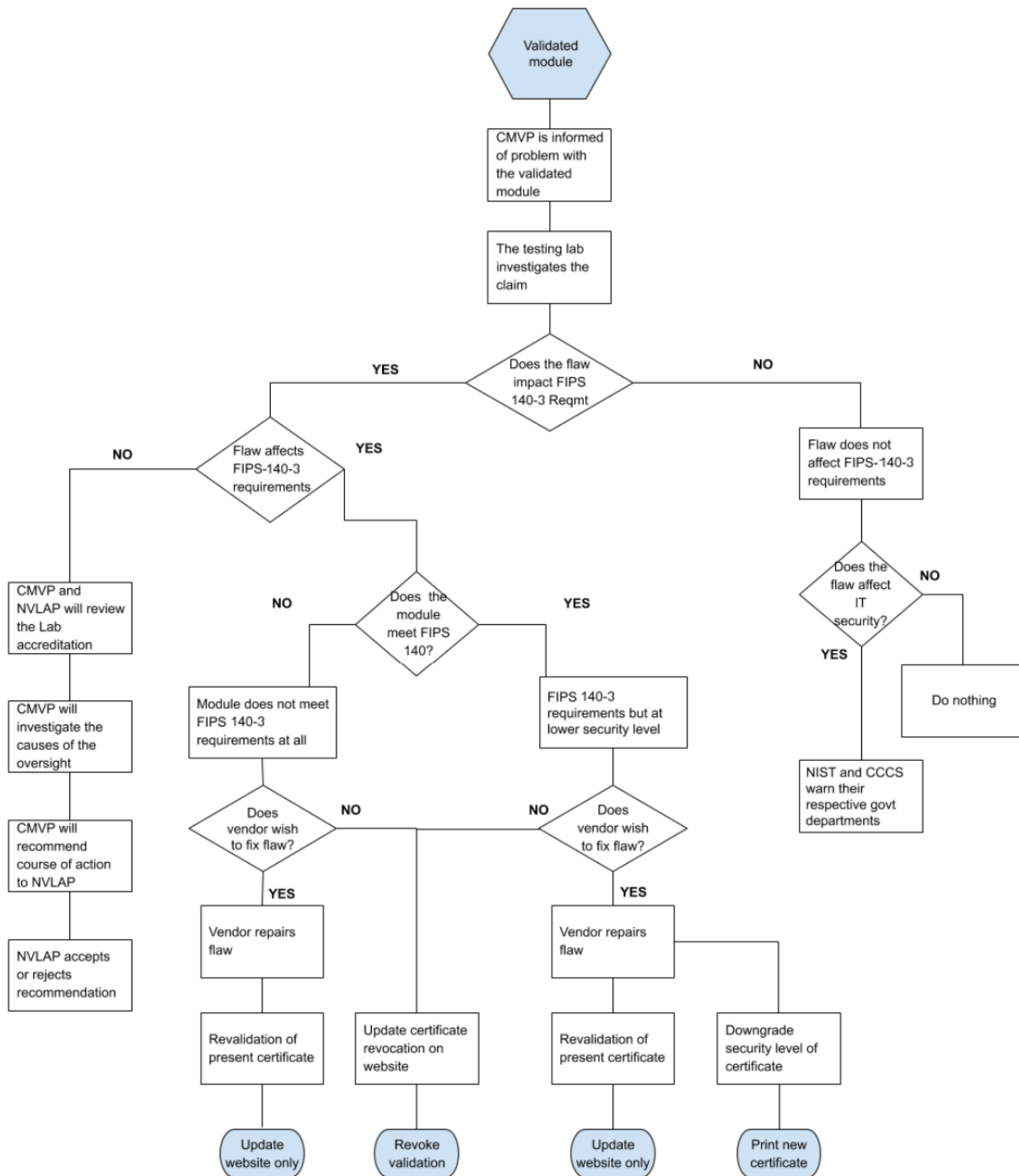
- 2480 module **shall** be tested against all of the listed TEs for that category in Equivalency  
 2481 Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP website.
- 2482 o If a module claims equivalency in multiple categories in comparison to a fully tested  
 2483 module under the same validation, all of the required TEs for each claim equivalency  
 2484 category **shall** be satisfied.
- 2485 - Focused Testing (FT) for Equivalency Category X:
- 2486 o The use of some technologies may introduce Security Relevant differences that cannot be  
 2487 predicted by this Section 7.10. For example, Programmable Logic Devices may be used  
 2488 to support the Cryptographic Module in a number of different ways that are security  
 2489 relevant (e.g., authentication). It is up to the lab to determine what section of the standard  
 2490 is affected by this security relevant difference and apply the Revalidation Regression Test  
 2491 Table found under the FIPS 140-3 Resources Tab of the CMVP website. For other  
 2492 sections not affected by this difference, Regression Testing per Equivalency Regression  
 2493 Test Table found under the FIPS 140-3 Resources Tab of the CMVP website shall be  
 2494 performed.
- 2495 - Complete Regression Testing (CRT): If an equivalency justification cannot be made, or the  
 2496 module differences can be mapped to a CRT entry within Equivalency Categories Tables  
 2497 under the FIPS 140-3 Resources Tab of the CMVP website, all modules, which lack an  
 2498 equivalency justification must, according to their security level, satisfy each TE listed in the  
 2499 Revalidation Regression Test Table under the FIPS 140-3 Resources Tab of the CMVP  
 2500 website.
- 2501 In each report where the vendor wishes to claim equivalency, the lab **shall**:
- 2502 - List the Equivalency Category, and specific component types being claimed in TE02.15.01.  
 2503 The lab must justify the component categorizations. The assumption is that the vendor  
 2504 initiated the Equivalency Category argument while the lab performed the analysis.
- 2505 - List the additional testing performed (if any) between the modules. This list **shall** be  
 2506 provided as an addendum to the test report.
- 2507 - Include in the Test Report how each module meets the TE's that are required for testing per  
 2508 this Section 7.10.
- 2509 For example:
- 2510 - Two devices to be on the same certificate have Hard Drives with different storage capacities,  
 2511 so testing requirement is Analysis Only, e.g., proof that both modules exist as claimed by the  
 2512 vendor.
- 2513 - Two devices to be on the same certificate have different types of Solid State Memory: one  
 2514 has NOR Flash and the other has NAND. This will require a small selection of testing, per  
 2515 Equivalency Regression Test Table found under the FIPS 140-3 Resources Tab of the CMVP  
 2516 website.
- 2517 - Two devices to be on the same certificate have different types of storage: one has a Hard  
 2518 Disk and the other has a Solid-State Drive. This will require complete regression testing per  
 2519 Revalidation Regression Test Table.

## 2520 Additional Comments

- 2521 - The lab **shall** perform full testing on at least one module.
- 2522 - This only applies to Operational testing of Hardware modules
- 2523 - Physical security testing (ISO/IEC 19790:2012, section 7.7) is not addressed for Security  
2524 Level 2 and above. In other words, this does not exempt the lab from performing physical  
2525 security testing for modules at Level 2 or above. This is because the lab needs to examine  
2526 each module for, e.g., opacity and tamper evidence, if there are physical differences between  
2527 the modules.
- 2528 - Components considered equivalent may still affect the entropy generated within the modules  
2529 in different ways. This must be accounted for in the entropy report, if entropy is applicable.
- 2530 - Equivalency considerations of the main processors/CPU's are out of scope of this Section  
2531 7.10. If the CPU is different between modules on the same certificate, then the full  
2532 Revalidation Regression Test Table must be run (found under the FIPS 140-3 Resources Tab  
2533 of the CMVP website). If the entropy is OE based, the entropy must address the new OE.
- 2534 - ISO/IEC 24759:2017 Section 6.7 Physical Security, Section 6.8 Non-Invasive Security and  
2535 Section 6.12 Mitigation of Other Attacks are not applicable.
- 2536

2537 **Annex A CMVP Post Validation Issue Assessment Process**

2538 **Annex A.1 Addressing Security Relevant Issues**



2539

2540 *Figure 5- Annex A. Validation Issue Assessment Process*

## 2541 **Annex A.2 Addressing CVE Relevant Vulnerabilities**

2542 The list of CVEs is maintained by NIST in the NVD at <https://nvd.nist.gov/>. The purpose of the  
2543 Scenario CVE revalidation (described in Section 7.1) is to provide the vendor a means to quickly  
2544 fix, test and revalidate a module that is subject to a security-relevant CVE, while at the same  
2545 time providing assurance that the module still meets the current FIPS 140 standards.

2546 Vendors must reference this database and address the security relevant CVE's that are within the  
2547 boundary of the module, not only during the validation process, but also after the module has  
2548 been validated. Without published security relevant CVEs being addressed by the vendor and  
2549 verified by the testing laboratory, the CMVP has no assurance that the module meets the  
2550 requirements to obtain or maintain validation.

2551 At the discretion of the CMVP, certificates will be revoked that do not comply. It is the goal of  
2552 the CMVP to maintain the security of validated modules.

2553 For more information about CVEs please also refer to <https://cve.mitre.org/>. See also [IG 11.A](#)  
2554 [CVE Management](#) for more guidance on this topic.

2555 **ACRONYMS**

2556	<b>ACVTS</b>	Automated Cryptographic Validation Testing System
2557	<b>ANSI</b>	American National Standards Institute
2558	<b>AS</b>	Assertion
2559	<b>CAVP</b>	Cryptographic Algorithm Validation Program
2560	<b>CCCS</b>	Canadian Centre for Cyber Security
2561	<b>CMVP</b>	Cryptographic Module Validation Program
2562	<b>CMUF</b>	Cryptographic Module User Forum
2563	<b>CR</b>	Cost Recovery
2564	<b>CSTL</b>	Cryptographic and Security Testing Laboratory
2565	<b>CVC</b>	Consolidated Validation Certificate
2566	<b>CVE</b>	Common Vulnerabilities and Exposures
2567	<b>CVP</b>	Cryptographic Validation Program
2568	<b>DES</b>	Data Encryption Standard
2569	<b>ECR</b>	Extended Cost Recovery
2570	<b>ESV</b>	Entropy Source Validation
2571	<b>FIPS</b>	Federal Information Processing Standard
2572	<b>FISMA</b>	Federal Information Security Management Act
2573	<b>FSM</b>	Finite State Model
2574	<b>GC</b>	Government of Canada
2575	<b>HB</b>	Handbook
2576	<b>ID</b>	Identification
2577	<b>IG</b>	Implementation Guidance
2578	<b>ISO</b>	International Organization for Standardization
2579	<b>ITAR</b>	International Traffic in Arms Regulation
2580	<b>IUT</b>	Implementation Under Test
2581	<b>N/A</b>	Not Applicable
2582	<b>NIST</b>	National Institute of Standards and Technology
2583	<b>NVLAP</b>	National Voluntary Laboratory Accreditation Program
2584	<b>OE</b>	Operational Environment
2585	<b>OS</b>	Operating System
2586	<b>PDF</b>	Portable Document Format

2587	<b>RFG</b>	Request for Guidance
2588	<b>SP</b>	Special Publication
2589	<b>TE</b>	Tester Evidence
2590	<b>TID</b>	Tracking Identification Number
2591	<b>TR</b>	Test Requirements
2592	<b>URL</b>	Uniform Resource Locator
2593	<b>VE</b>	Vendor Evidence