

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date March 20, 2020

Original Release Date October 9, 2019

Superseding Document

Status Final

Series/Number NIST Special Publication 800-140F

Title CMVP Approved Non-Invasive Attack Mitigation Test Metrics:
CMVP Validation Authority Updates to ISO/IEC 24759

Publication Date March 2020

DOI <https://doi.org/10.6028/NIST.SP.800-140F>

CSRC URL <https://csrc.nist.gov/publications/detail/sp/800-140f/final>

Additional Information FIPS 140-3 Transition Effort

<https://csrc.nist.gov/projects/fips-140-3-transition-effort/fips-140-3-docs>

2

3 **CMVP Approved Non-Invasive**
4 **Attack Mitigation Test Metrics:**

5 *CMVP Validation Authority Updates to ISO/IEC 24759:2014(E)*

6

7

8

9

10

11

12

13

14

15

16

I N F O R M A T I O N S E C U R I T Y

17

18

Kim Schaffer

19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40

Draft NIST Special Publication 800-140F

**CMVP Approved Non-Invasive
Attack Mitigation Test Metrics:**

CMVP Validation Authority Updates to ISO/IEC 24759:2014(E)

Kim Schaffer
*Computer Security Division
Information Technology Laboratory*

October 2019



41
42
43
44
45
46
47
48

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary for Standards and Technology

49

Authority

50 This publication has been developed by NIST in accordance with its statutory responsibilities under the
51 Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law
52 (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including
53 minimum requirements for federal information systems, but such standards and guidelines shall not apply
54 to national security systems without the express approval of appropriate federal officials exercising policy
55 authority over such systems. This guideline is consistent with the requirements of the Office of Management
56 and Budget (OMB) Circular A-130.

57 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and
58 binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these
59 guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce,
60 Director of the OMB, or any other federal official. This publication may be used by nongovernmental
61 organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would,
62 however, be appreciated by NIST.

63 National Institute of Standards and Technology Special Publication 800-140F
64 Natl. Inst. Stand. Technol. Spec. Publ. 800-140F, 8 pages (October 2019)
65 CODEN: NSPUE2

66

67 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
68 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
69 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
70 available for the purpose.

71 There may be references in this publication to other publications currently under development by NIST in accordance
72 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,
73 may be used by federal agencies even before the completion of such companion publications. Thus, until each
74 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For
75 planning and transition purposes, federal agencies may wish to closely follow the development of these new
76 publications by NIST.

77 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to
78 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
79 <https://csrc.nist.gov/publications>.

80

81 **Public comment period: *October 9, 2019 through December 9, 2019***

82 National Institute of Standards and Technology
83 Attn: Computer Security Division, Information Technology Laboratory
84 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
85 Email: sp800-140-comments@nist.gov

86 All comments are subject to release under the Freedom of Information Act (FOIA).

87

Reports on Computer Systems Technology

88 The Information Technology Laboratory (ITL) at the National Institute of Standards and
89 Technology (NIST) promotes the U.S. economy and public welfare by providing technical
90 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test
91 methods, reference data, proof of concept implementations, and technical analyses to advance the
92 development and productive use of information technology. ITL's responsibilities include the
93 development of management, administrative, technical, and physical standards and guidelines for
94 the cost-effective security and privacy of other than national security-related information in federal
95 information systems. The Special Publication 800-series reports on ITL's research, guidelines, and
96 outreach efforts in information system security, and its collaborative activities with industry,
97 government, and academic organizations.

98

Abstract

99 NIST Special Publication (SP) 800-140F replaces the approved non-invasive attack mitigation
100 test metric requirements of ISO/IEC 19790 Annex F. As a validation authority, the
101 Cryptographic Module Validation Program (CMVP) may supersede this Annex in its entirety.
102 This document supersedes ISO/IEC 19790 Annex F and ISO/IEC 24759 paragraph 6.18.

103

Keywords

104 attack mitigation; Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS
105 140; ISO/IEC 19790; ISO/IEC 24759; non-invasive; testing requirement; vendor evidence;
106 vendor documentation.

107

108

Audience

109 This document is focused toward the vendors, testing labs, and CMVP for the purpose of
110 addressing issues in cryptographic module testing.

111 **Table of Contents**

112 **1 Scope..... 1**

113 **2 Normative references..... 1**

114 **3 Terms and definitions 1**

115 **4 Symbols and abbreviated terms 1**

116 **5 Document organization..... 2**

117 5.1 General..... 2

118 5.2 Modifications..... 2

119 **6 CMVP approved non-invasive attack mitigation test metric requirements ... 2**

120 6.1 Purpose 2

121 6.2 Approved non-invasive attack mitigation test metrics 2

122

1 Scope

124 This document specifies the Cryptographic Module Validation Program (CMVP) modifications
 125 of the methods to be used by a Cryptographic and Security Testing Laboratory (CSTL) to
 126 demonstrate conformance. This document also specifies the modification of methods for
 127 evidence that a vendor or testing laboratory provides to demonstrate conformity. Unless
 128 otherwise specified in this document, the test requirements are specified in ISO/IEC 24759
 129 paragraph 6.18.

2 Normative references

131 This section identifies additional references to the normative references cited in ISO/IEC 24759.
 132 For dated references (e.g., ISO/IEC 19790:2012/Cor.1:2015(E)), only the edition cited applies.
 133 For undated references (e.g., ISO/IEC 19790), the latest edition of the referenced document
 134 (including any amendments) applies.

135 National Institute of Standards and Technology (2019) *Security Requirements for*
 136 *Cryptographic Modules*. (U.S. Department of Commerce, Washington, DC), Federal
 137 Information Processing Standards Publication (FIPS) 140-3.
 138 <https://doi.org/10.6028/NIST.FIPS.140-3>

3 Terms and definitions

140 The following terms and definitions supersede or are in addition to ISO/IEC 19790 and ISO/IEC
 141 24759.

142 *No additional terms at this time.*

4 Symbols and abbreviated terms

144 The following symbols and abbreviated terms supersede or are in addition to ISO/IEC 19790 and
 145 ISO/IEC 24759 throughout this document:

146	CCCS	Canadian Centre for Cyber Security
147	CMVP	Cryptographic Module Validation Program
148	CSD	Computer Security Division
149	CSTL	Cryptographic and Security Testing Laboratory
150	FIPS	Federal Information Processing Standard
151	FISMA	Federal Information Security Management/Modernization Act

152	NIST	National Institute of Standards and Technology
153	SP 800-XXX	NIST Special Publication 800 series document
154	TE	Test Evidence
155	VE	Vendor Evidence

156 **5 Document organization**

157 **5.1 General**

158 Section 6 of this document replaces the approved non-invasive attack mitigation test metrics
159 requirements of ISO/IEC 19790 Annex F and ISO/IEC 24759 paragraph 6.18.

160 **5.2 Modifications**

161 Modifications will follow a similar format as in ISO/IEC 24759. For additions to test
162 requirements, new Test Evidence (TEs) or Vendor Evidence (VEs) will be listed by increasing
163 the “sequence_number.” Modifications can include a combination of additions using underline
164 and deletions using ~~striketrough~~. If no changes are required, the paragraph will indicate “No
165 change.”

166 **6 CMVP-approved non-invasive attack mitigation test metric requirements**

167 **6.1 Purpose**

168 This document identifies CMVP-approved non-invasive attack mitigation test metrics.

169 **6.2 Approved non-invasive attack mitigation test metrics**

170 ISO/IEC 17825 Information technology – Security techniques – Testing methods for the
171 mitigation of non-invasive attack classes against cryptographic modules

172 ISO/IEC 20085-1 Information technology – Security techniques – Test tool requirements and test
173 tool calibration methods for use in testing non-invasive attack mitigation techniques in
174 cryptographic modules — Part 1: Test tools and techniques (pending publication)

175 ISO/IEC 20085-2 Information technology – Security techniques – Test tool requirements and test
176 tool calibration methods for use in testing non-invasive attack mitigation techniques in
177 cryptographic modules — Part 2: Test calibration methods and apparatus. (pending publication)

178 **Document Revisions**

Date	Change

179

180