

3 **CMVP Approved Non-Invasive**
4 **Attack Mitigation Test Metrics:**
5 *CMVP Validation Authority Updates to ISO/IEC 24759*

6
7 Kim Schaffer
8
9
10

11 This publication is available free of charge from:
12 <https://doi.org/10.6028/NIST.SP.800-140Fr1-draft>
13
14
15
16
17
18
19
20
21

22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52

Draft NIST Special Publication 800-140F
Revision 1

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

Kim Schaffer
*Computer Security Division
Information Technology Laboratory*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-140Fr1-draft>

August 2021



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology*

53

Authority

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

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

67 National Institute of Standards and Technology Special Publication 800-140F Revision 1
68 Natl. Inst. Stand. Technol. Spec. Publ. 800-140F Rev. 1, 8 pages (August 2021)
69 CODEN: NSPUE2

70 This publication is available free of charge from:
71 <https://doi.org/10.6028/NIST.SP.800-140Fr1-draft>

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

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

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

85 **Public comment period: August 20, 2021 – September 20, 2021**

86 National Institute of Standards and Technology
87 Attn: Computer Security Division, Information Technology Laboratory
88 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
89 Email: sp800-140-comments@nist.gov

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

91 **Reports on Computer Systems Technology**

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

102 **Abstract**

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

107 **Keywords**

108 attack mitigation; Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS
109 140; ISO/IEC 19790; ISO/IEC 24759; non-invasive; testing requirement; vendor evidence;
110 vendor documentation.

111 **Audience**

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

114
115
116
117
118
119
120
121
122
123
124
125
126
127
128

Table of Contents

1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	1
5	Document organization	2
5.1	General	2
5.2	Modifications	2
6	CMVP-approved non-invasive attack mitigation test metric requirements ...	2
6.1	Purpose	2
6.2	Approved non-invasive attack mitigation test metrics	2
	Document Revisions	3

1 Scope

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

2 Normative references

This section identifies the normative references cited as ISO/IEC 19790 and ISO/IEC 24759. The specific editions to be used are ISO/IEC 19790:2012 and ISO/IEC 24759:2017. Please note that the version 19790:2012 referenced here includes the corrections made in 2015.

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

3 Terms and definitions

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

No additional terms at this time.

4 Symbols and abbreviated terms

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

151	CCCS	Canadian Centre for Cyber Security
152	CMVP	Cryptographic Module Validation Program
153	CSD	Computer Security Division
154	CSTL	Cryptographic and Security Testing Laboratory
155	FIPS	Federal Information Processing Standard
156	FISMA	Federal Information Security Management/Modernization Act
157	NIST	National Institute of Standards and Technology

158 SP 800-XXX NIST Special Publication 800 series document

159 **5 Document organization**

160 **5.1 General**

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

163 **5.2 Modifications**

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

169 **6 CMVP-approved non-invasive attack mitigation test metric requirements**

170 **6.1 Purpose**

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

172 **6.2 Approved non-invasive attack mitigation test metrics**

- 173 1. International Organization for Standardization/International Electrotechnical
174 Commission. *ISO/IEC 17825 – Information technology – Security techniques – Testing*
175 *methods for the mitigation of non-invasive attack classes against cryptographic modules*
- 176 2. International Organization for Standardization/International Electrotechnical
177 Commission. *ISO/IEC 20085-1 – IT Security techniques – Test tool requirements and test*
178 *tool calibration methods for use in testing non-invasive attack mitigation techniques in*
179 *cryptographic modules — Part 1: Test tools and techniques*
- 180 3. International Organization for Standardization/International Electrotechnical
181 Commission. *ISO/IEC 20085-2 – IT Security techniques – Test tool requirements and test*
182 *tool calibration methods for use in testing non-invasive attack mitigation techniques in*
183 *cryptographic modules — Part 2: Test calibration methods and apparatus*

184

Document Revisions

Edition	Date	Change
Revision 1	[date]	§ 6.2 Approved non-invasive attack mitigation test metrics Added: ISO/IEC 17825 and associated ISO/IEC 20085-1 and -2

185