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

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

National Institute of Standards and Technology
U.S. Department of Commerce

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

Authority

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

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

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

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

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

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

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

Reports on Computer Systems Technology

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

Abstract

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

Keywords

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

Audience

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

Table of Contents

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:

CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CSD	Computer Security Division
CSTL	Cryptographic and Security Testing Laboratory
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management/Modernization Act
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 ~~strikethrough~~. 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*

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