Keywords: anti-malware; protocol; standard; test

AMTSO 1:2017a
November 16, 2017

DRAFT 6.1

Testing Protocol
Standards for the Testing of
Anti-Malware Solutions

Sponsored by:

The Anti-Malware Testing Standards Organization, Inc.
AMTSO Member Approval Date (2017-12-05 APPROVED DRAFT)

Abstract:

This Standard provides testing protocol and behavior expectations for testers and vendors relating to the testing of anti-malware solutions. It specifies the information to communicate and how that information should be communicated between testers and vendors with products or solutions that may be included in public and private tests. Separate sections on referenced publications, definitions, standards elements, and arrangements are included.

www.amtso.org

Notice and Disclaimer of Liability Concerning the Use of AMTSO Documents

This document sets forth the draft testing protocol standard ("Standard") for the testing of anti-malware solutions. This Standard was developed and is published by the Anti-Malware Testing Standards Organization, Inc., and compliance with this Standard is a requirement for confirmation of compliance of a Test by AMTSO.

This Standard has been developed by AMTSO to help drive transparent and fair testing in the anti-malware industry, and has been adopted by AMTSO members in draft form. **The submission of an application for confirmation of compliance of a Test does not guarantee that the Test will be confirmed compliant, which will be done only in AMTSO's sole discretion. Moreover, confirmation of compliance of a Test by AMTSO under this Standard is not an endorsement by AMTSO of the Test, or of any one or more anti-malware products, but rather is a confirmation that the Test complies with this Standard.**

AMTSO is supplying this information for general educational purposes only. No engineering or any other professional services are being provided. You must use your own professional skill and judgment when reviewing this document and rather than solely relying on the information provided herein.

AMTSO believes that the information in this document is accurate as of the date of publication although it has not verified its accuracy, and is not guaranteeing it is free of errors. Further, such information is subject to change without notice and AMTSO is under no obligation to provide any updates or corrections.

YOU UNDERSTAND AND AGREE THAT THIS DOCUMENT IS PROVIDED TO YOU EXCLUSIVELY ON AN AS-IS BASIS WITHOUT ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS, IMPLIED, OR STATUTORY. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, AMTSO EXPRESSLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, CONTINUOUS OPERATION, COMPLETENESS, QUALITY, ACCURACY, AND FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL AMTSO BE LIABLE FOR ANY DAMAGES OR LOSSES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, LOST DATA, OR BUSINESS INTERRUPTION) ARISING DIRECTLY OR INDIRECTLY OUT OF ANY USE OF THIS DOCUMENT INCLUDING, WITHOUT LIMITATION, ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, AND PUNITIVE DAMAGES REGARDLESS OF WHETHER ANY PERSON OR ENTITY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document is protected by AMTSO's intellectual property rights and may be additionally protected by the intellectual property rights of others.

Foreword

This Standard was developed to provide guidance to anti-malware testers and vendors, and any others involved in the testing or rating of anti-malware products and solutions. This Standard includes a testing protocol that can be used by any entity or individual whose professional or private activities are relevant to the subject addressed. Compliance with this Standard conforms to the principles and practices of AMTSO's Fundamental Principles of Testing.

AMTSO is a non-profit organization established to help improve the business conditions related to the development, use, testing, and rating of anti-malware solutions. Anti-malware testing is the critical link between the vendor and end user, and transparent and fair testing can establish that anti-malware solutions work as vendors claim. However, opaque or unfair testing can create misleading results and leave corporations and consumers with inadequate protection that risks both their privacy and security. In addition, the lack of proper testing protocols can create unnecessary expense for vendors, which ultimately can impact the amount of resources devoted to research and development, and shift focus from critical threat detection toward compliance with opaque or unfair testing procedures.

A key part of AMTSO's mission has been to establish protocols relating to testing behavior within the industry. In 2008, AMTSO adopted principles for testing that have been widely adopted as best practices for anti-malware testers. However, these general principles did not provide the structure necessary to improve testing conditions on a global scale. To solve this problem, AMTSO has driven a cross-industry effort to develop globally applicable testing standards and a related compliance program. This Standard is based on a premise that although testers and vendors must retain their independence, anti-malware testing is more likely to be transparent and fair if there is communication between the parties regarding the solution being tested, and the testing methodology. We believe that this Standard and the AMTSO compliance program have the potential to create a higher level of customer trust through more transparent and fair testing, and improved industry behavior.

Suggestions for improvement of this Standard are welcome. They should be sent to the Chairperson of the AMTSO Standards Committee via email to: standards@amtso.org.

AMTSO Standards Committee

The following members of AMTSO's Standards Committee participated in the development of this Standard. The affiliated organizations are listed to demonstrate the openness and balance of the committee. Approval of this Standard by the individuals listed does not imply endorsement of their affiliated organization.

Name of Representative	**Affiliation**
Andreas Clementi	*AV-Comparatives*
Andreas Unterpertinger	*AV-Comparatives*
Bhaarath Venkateswaran	*NSS Labs*
Brad Albrecht	*CrowdStrike*
Chad Skipper	*Cylance*
Dennis Batchelder	*AppEsteem*
Evgeny Vovk	*Kaspersky Lab*
Glaucia Young	*Microsoft*
Jaimee King	*AppEsteem*
Jimmy Astle	*Carbon Black*
Jiri Sejtko	*AVAST*
John Hawes	*AMTSO*
Mark Kennedy	*Symantec*
Onur Komili	*Sophos*
Peter Stelzhammer	*AV-Comparatives*
Samir Mody	*K7 Computing*
Sam Curry	*Cybereason*
Scott Jeffreys	*AMTSO*
Scott Marcks	*Cylance*
Simon Edwards	*SE Labs*

Contents

Testing Protocol Standards for the Testing of Anti-Malware Solutions

Important Notice: This AMTSO Standard establishes process guidelines for transparency and fairness in the testing process. It is not intended to, nor does it, assure the accuracy of test results or ensure the security of any party, or legal compliance with any federal, state, or local restriction or law.

1. Overview

1.1. Scope

This Standard includes testing protocols and compliance for Testers and Vendors. AMTSO will offer confirmation of compliance for publicly-released Tests that successfully demonstrate compliance with this Standard. Although Private Tests will not be confirmed compliant by AMTSO under this Standard, all Testers and Vendors may benefit by following these testing protocols for any Public or Private Test.

1.2. Purpose

AMTSO recognizes the need for independent product testing to help end users adequately understand the differences in security products, and to validate Vendors' claims in the market. Transparent and fair product testing is the cornerstone to achieving this goal, and we believe that Testing is more effective with the cooperation and participation of both Testers and Vendors. Therefore, the purpose of this Standard is to help improve the transparency and fairness of Anti-Malware Tests that are made publicly available. Additional purposes include:

- Providing Testers with fair access to Products as they run Tests they intend to accredit
- Encouraging more voluntary participation by Vendors
- Establishing methods for Vendor notification
- Supporting disclosure of provenance, Curation strategy, and prior access to Test samples
- Establishing processes for feedback, auditing, disputes, and conflict resolution
- Encouraging real-world scientific tests that are verifiable, statistically valid, and objective.

This Standard serves as the foundation for the AMTSO testing compliance program, which has been established to help ensure the reliability of compliance assertions made in connection with Anti-Malware testing.

1.3. Legal Compliance

Each implementer of this Standard, including Testers and Participants (whether Voluntary or not), is required to understand and comply with all applicable rules and regulations when performing its obligations and exercising its rights herein including, without limitation, all applicable privacy, data protection and antitrust laws and regulations.

2. Informative References, Definitions, and Acronyms

2.1. Informative References

2.1.1. The following documents, in whole or in part, are referenced in this document and are important for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.1.1.1. AMTSO - Best Practices for Dynamic Testing

2.1.1.2. AMTSO - Best Practices for Testing In-the-Cloud Security Products

2.1.1.3. AMTSO - Guidelines for Testing Protection Against Targeted Attacks

2.1.1.4. AMTSO - Guidelines on Facilitating Testability

2.1.1.5. AMTSO - Guidelines to False Positive Testing

2.1.1.6. AMTSO - Issues Involved in the "Creation" of Samples for Testing

2.1.1.7. AMTSO - Performance Testing Guidelines

2.1.1.8. AMTSO - Sample Selection for Testing

2.1.1.9. AMTSO - Suggested Methods for the Validation of Samples

2.1.1.10. AMTSO – The Fundamental Principles of Testing

2.1.1.11. AMTSO - Whole-Product Testing Guidelines

2.2. Definitions

2.2.1. **AMTSO Member**. Individual or entity that has been accepted as a member of AMTSO and has met the current requirements for membership, including payment of annual membership fees.

2.2.2. **Anti-Malware**. Products and services that claim to prevent, detect, or remediate Malware. Anti-Malware solutions may offer standalone protection, or may be incorporated into suites of products and services.

2.2.3. **Business Days**. For the purposes of this Standard, a Business Day is Monday through Thursday, not including observed holidays in applicable countries.

2.2.4. **Classification**. The designation given to a sample.

2.2.5. **Cloud**. The term's "Cloud" and "in the Cloud" refer, respectively, to the internet (or other resources external to a protected system) and to resources and technologies run or served from there –

online detection databases, reputation systems, black- and white-lists, managed services, and so on.

2.2.6. **Collection**. The process of gathering the files, URLs, or other objects to be used as samples in Tests. Collection also is used to refer to the group of collected samples.

2.2.7. **Commencement Date of a Test.** The specific date when a Test was considered to start, as defined by the Tester.

2.2.8. **Commentary.** The posted opinion of a Participant on a Test Plan or the Test results, as submitted by Participants for inclusion on the AMTSO website in connection to a Test.

2.2.9. **Conviction.** The process of confirming that a given sample or Test Case represents a valid threat, and therefore is suitable for inclusion in a Test. Conviction is part of the overall Curation process.

2.2.10. **Curation**. The sourcing, Classifying, validating, and possible Convicting processes for handling Samples.

2.2.11. **Dispute Process**. The process in which Testers provide Participants with evidence on their Product's performance in a Test and give them an option to review this evidence to determine whether they agree with the Tester's findings.

2.2.12. **Fair**. The term "Fair" is used with its standard meaning of treating all equally without bias or discrimination. AMTSO particularly emphasizes the following aspects of Fairness:

- Fair Opportunity: accept actions equally from all Participants to ensure a level playing field. All Participants have the ability to gain access to the same rights.
- Fair Disclosure: the testing process does not have any undisclosed material conflicts of interest, and proactive disclosures are made by the Tester when any such conflicts are known.
- Fair Commentary: the ability to provide comment on items and express opinion without the fear of retribution from one or multiple parties.

Anything not fulfilling the above requirements, or otherwise in violation of Section 1.3 herein, is considered "unfair".

2.2.13. **Feedbac**k Process. See Dispute Process.

2.2.14. **Informative Reference**. Elements of this Standard that are descriptive – Informative References are used to help the reader understand the Normative Reference elements.

2.2.15. **Malware**. Malware includes software or other electronic data capable of infiltrating or damaging a computer system or user data, or misleading users.

2.2.16. **Normative Reference**. Elements of this Standard that are prescriptive – they must be followed to comply with this Standard.

2.2.17. **Participant**. A Vendor that represents a Product included in a Test.

2.2.18. **Private Test**. An Anti-Malware Test where the Tester and its Participants have no intent to publish or publicly reference the Test's existence or results.

2.2.19. **Product**. An Anti-Malware solution. All Products have the potential to be tested.

2.2.20. **Public Test**. An Anti-Malware test where the Tester or its Participants intend to publish or publicly reference its existence or its results.

2.2.21. **Standard.** Testing protocol requirements, specifications, recommended practices, and guidelines, published in accordance with established procedures.

2.2.22. **Tests.** Used inclusively to refer to Public Tests and/or Private Tests.

2.2.23. **Test Case.** A set of conditions that a Tester uses to measure a Product.

2.2.24. **Test Plan**. A plan, provided by a Tester, that complies with Section 6 of this standard.

2.2.25. **Tester**. An individual or entity that conducts Tests on Anti-Malware Products to establish functionality, effectiveness, comparative results, compliance, or other determinations.

2.2.26. **Vendor**. An organization or individual that offers Anti-Malware Products.

2.2.27. **Voluntary Participant**. A Participant who has chosen to cooperate with the Tester on the Test in the manner designated in the Test Plan, and has complied with the Voluntary Participant requirements set forth in Section 7 below.

2.3. Acronyms

2.3.1. **AMTSO:** The Anti-Malware Testing Standards Organization, Inc.

2.3.2. **SWG:** The Standards Working Group within AMTSO.

3. AMTSO Contact List

3.1. Vendors that have any Product that may be included in any Public Test, and Testers that intend to conduct any Public Test, should provide up-to-date contact information to AMTSO for inclusion on the AMTSO Contact List.

3.1.1. The AMTSO Contact List shall be hosted on the amtso.org website and shall be maintained by AMTSO.

3.1.1.1. To provide a contact, Vendors and Testers should submit their information via the AMTSO Contact List portal located on AMTSO's public web site.

3.1.1.2. The provided contact may be an email alias that includes a series of persons from one particular Vendor or Tester. However, each Vendor and Tester that includes such an alias is responsible for maintaining such alias and obtaining any necessary consents for inclusion on the list.

3.1.1.3. It is the responsibility of the submitting party to ensure their contact information

is current. AMTSO shall not be responsible for the accuracy of contact information provided by any Vendor or Tester. The information can be updated through the AMTSO Contact List portal.

3.1.1.4. A Vendor or Tester does not need to be an AMTSO Member to include their contact information on the AMTSO Contact List.

3.1.1.5. The AMTSO Contact List shall only be available to Vendors and Testers that have provided their current contact information to the AMTSO Contact List.

3.1.1.6. Vendors and Testers shall protect the Contact List from disclosure to any third-party, and understand that the Contact List is maintained and provided on the AMTSO website under the AMTSO Terms of Use.

3.2. Testers may rely on information provided in the AMTSO Contact List, and shall not be responsible to take further efforts to provide proper notification beyond the information in the AMTSO Contact List.

3.2.1 *Informative Reference:* If a Vendor's contact information is not found or is incorrect, AMTSO encourages Testers to report this to AMTSO, so AMTSO can attempt to obtain or correct contact information.

4. Notification of Test Plan

4.1. Testers shall provide notification of a Test Plan to all potential Participants.

4.1.1. *Informative Reference*: Sending notification directly to the potential Participants through use of contact information included on the AMTSO Contact List described in Section 3, or through public notification of the Test Plan in compliance with Section 5 herein, is considered notification.

4.2. A Tester that provides public notification on the AMTSO website shall meet its obligation for public notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test.

4.3. For each Test, at least one Test Plan notification shall be made no more than two (2) calendar months, and no less than five (5) Business Days, before the Commencement Date of a Test.

5. Public Test Notification Requirements

5.1. If a Tester has opted to provide public notification of the Test Plan, the Tester shall post the Test Plan on the AMTSO website.

5.1.1. To support public notification of Test Plans, AMTSO shall provide a general email notification to all Vendors registered on the AMTSO Contact List.

5.2. Testers that provide direct notification to potential Participants through use of contact information on the AMTSO Contact List shall provide notification to all potential Participants at approximately the same time. This is to ensure that no potential Participants are provided significant advance notice over other potential Participants, thus keeping the notification periods similar.

5.3. The Test Plan shall be either a single plan for a single Test, or a plan that covers multiple potential Tests with potentially different combinations of Vendors.

5.4. All potential Participants are encouraged to provide their Product as requested by any Tester, whether it be freely provided, provided for cost, or otherwise.

5.4.1. Potential Participants may notify the Tester that they do not want their Product included in the Test. The Tester is not required to comply with this request.

6. Test Plan Requirements

6.1. The Test Plan shall include the following information:

6.1.1. A stated intent by the Tester to follow this AMTSO Standard.

6.1.1.1. *Informative Reference*. AMTSO encourages Testers to follow through on any commitment to comply with this Standard, and Vendors to follow through on any commitment to be Voluntary Participants, to avoid the break-down of good faith between Vendors and Testers.

6.1.2. The types of Products that are intended be included in the Test.

6.1.3. The purpose of the Test, including the type(s) of threats the Products will be tested against.

6.1.4. The Commencement Date of the Test, or a range of dates during which the Test may commence.

6.1.5. If the Test Plan requires Vendors to perform any specific actions to participate, the Test Plan shall provide a schedule with dates or ranges of dates for each required Vendor action.

6.1.5.1. *Informative Reference*: The Test Plan may need to provide dates to ensure that the Tester has access to an appropriate version of a Product.

6.1.5.2. *Informative Reference*: The Test Plan should take into account observed holidays in relevant countries as they request actions from Vendors.

6.1.6. A clear definition of the methodology of the Test, which shall include a description of the testing environment and what the Test is intending to achieve;

6.1.6.1. *Normative Reference*: AMTSO Fundamental Principles of Testing: Principle 6: Testing methodology must be consistent with the testing purpose.

6.1.7. A statement of intention of Product versions, configurations to be applied, and which functionality of the Products will be tested.

6.1.7.1. *Informative Reference*. When running Products over long periods of time, version information may not be available or may change as various components are updated. Testers should provide a policy of how this will be handled as part of the Test's methodology in the Test Plan. AMTSO

6.1.8. An overview of the Test's scoring and certification plan.

6.1.9. Instructions on how the Test's results can be disputed.

6.1.10. Instructions on how a Vendor may become a Voluntary Participant with respect to each Product that is intended to be included in the Test.

6.1.10.1. A Tester shall provide all Participants with the option to be Voluntary Participants, as set forth in Section 7. A Test may still comply with this Standard if only some, or none, of the Participants accept the option to become Voluntary Participants.

6.1.10.1.1. *Informative Reference*: AMTSO's desire is that any Participant should want to, and have the ability to, be a Voluntary Participant.

6.1.10.2. A Tester may charge for Participation in a Test, and may charge for services available only to Voluntary Participants, but shall not charge additional fees for Participants to be Voluntary.

6.1.10.2.1. *Informative Reference*: AMTSO's goal with having Voluntary Participants is that in exchange for cooperating (engaging with Testers and following disclosure requirements), Voluntary Participants have additional rights to audit their configuration and provide commentary on Test results. There must be no additional cost to Participants to be Voluntary.

6.1.10.2.2. *Informative Reference:* If a Tester charges to participate in a Public Test or any related services, and a Participant chooses to not pay the fee, that Participant must be able to choose to be a Voluntary Participant and follow this AMTSO Standard.

6.1.11. A reasonable amount of information on sample provenance and sample Collection strategy.

6.1.11.1. *Informative Reference.* The Tester should provide sufficient information for the Participant to understand why the samples are relevant, but not so much information as to be administratively burdensome for the Tester or allow Participants to unfairly influence their results.

6.1.11.2. *Informative Reference.* The Tester should utilize a Curation approach that does not allow any Participant to unfairly influence their results.

6.1.12. A clear description of how samples will be Curated, and how and when feedback will be solicited and processed and what evidence will be provided. Testers may limit Vendor participation in sample Curation to only include Voluntary Participants. If this limitation is provided, then all Voluntary Participants must be given equal opportunities to participate in such Curation and feedback processes for all their respective Products.

6.1.12.1. *Informative Reference*. Testers should select only samples and Test Cases which can be provided to Participants for independent validation, or for which all Participants can be provided with both adequate evidence of accurate Curation, and adequate information to enable the Participant

to remediate any shortcomings in their Product.

6.1.12.2. *Informative Reference*: Testers must be clear on the approach they will use to ensure relevancy of the samples. This is not intended for the Tester to disclose their confidential information, or to allow Participants to unfairly influence their test results.

6.1.12.3. *Informative Reference*: The Test Plan may include a requirement that any disputes from a Participant must be accompanied by an element of proof, or evidence that the dispute is legitimate, rather than just the Participant's statement of disagreement.

6.1.12.4. *Informative Reference*: If Tester includes Products which were identified by a Vendor as having a restricted geographic distribution, the Tester should include a statement of geographic relevance of their samples.

6.2. The Test Plan may provide Vendors the option to opt out of a Public Test. If the Test Plan includes this option and a Vendor chooses to opt out, the Tester shall not include the Vendor in that specific Test.

6.2.1. *Informative Reference*. In the interests of clarity, Testers are not required to include an opt out provision in any Test Plan; however, if they do include this option, they must honor a Vendor request to opt out.

6.3. The Test Plan may include instructions for potential Participants to provide Specific Data regarding the Product(s) to be included in the test. Some examples of this include:

- Disclosure for each Product included in the test of the types of data being transmitted to the Cloud.
- A means for confirming whether a Product's cloud connectivity or other features are functioning.

- Instructions for enabling logging within the Product

6.4 Testers must notify all Participants of any significant changes to previously communicated Test Plans.

6.4.1 *Informative Reference*: "Significant changes" include any changes materially affecting the rights granted to Voluntary Participants, or changes to the Commencement Date of a Test moving that date outside the notification requirements in Section 4.3.

7. Voluntary Participants

In response to the Test Plan, all Vendors may choose to become a Voluntary Participant by providing notification to the Tester in the manner designated in the Test Plan and complying with the requirements in Section 7.1.

7.1. A Voluntary Participant shall provide the following disclosures (disclosure requirements) to the Tester:

7.1.1. The Specific Data, defined in Section [6.3] above.

7.1.2. Any existing Product feature either specifically designed to preclude accurate testing or that the Vendor knows has that effect.

7.1.3. Any known or anticipated "variances" between the Product acquired or submitted to the Tester for inclusion in the Test, and the Product that will be provided to the typical end user.

7.1.3.1. "Variances" shall include all non-routine changes or configurations to a Product, that causes a material difference between the Product that has been included in a Test, and that which is provided to the end user. "Variances" do not include any routine Product updates or upgrades.

7.1.3.1.1. *Informative Reference.* This definition is intended to also address the "Golden Sample" issue, in which Products may be provided for testing that are not representative of the Product that will be provided in actual production and delivery to the end user.

7.1.4. Any material conflict of interests or other information that could materially impact the reliability of the test.

7.1.4.1. *Informative Reference.* Definition of Conflict of Interest: "A conflict of interest is a situation in which financial or other personal considerations have the potential to compromise or bias professional judgment and objectivity. An "apparent conflict of interest" is one in which a reasonable person would think that the professional's judgement is likely to be compromised. A "potential conflict of interest" involves a situation that may develop into an actual conflict of interest. Please note that the existence of a conflict of interest does not mean that there is any misconduct. Misconduct in testing is limited to fabrication, falsification, and plagiarism. A conflict of interest only implies the potential for bias, not a likelihood."[1]

7.1.5. Any unlicensed third-party intellectual property in the Product being tested.

7.1.5.1. A Tester may rely on the assertion or omission of a Voluntary Participant regarding the use of any third-party intellectual property included in the Product to be tested.

7.2. In completing the disclosure requirements, a Voluntary Participant may provide an "exceptions" list, identifying specific disclosed items that are precluded from public disclosure.

7.2.1. *Informative Reference*. The "exceptions" list is meant to provide a method for a Voluntary Participant to provide information to the Tester that is protected by confidentiality. In general, any information the Tester discovers regarding the tested Product may be made part of the Tester's public test results. The intention with this provision is to encourage open and honest disclosure by the Voluntary Participant to improve the potential for accurate test results.

7.3. Voluntary Participants and Testers shall provide "timely", "relevant", and "Fair" responses to inquiries from each other.

7.3.1. A "timely" response shall be provided within five (5) Business Days of the receipt of the request.

[1] http://ori.hhs.gov/education/products/columbia_wbt/rcr_conflicts/foundation/

7.3.2. A “relevant” response shall be one that directly addresses the subject of the request.

7.3.3. A “Fair” response shall meet the requirements of Fair Commentary as described in Section 2.

7.4. Voluntary Participants shall provide the Tester with a complete and executed Voluntary Participant Attestation, in substantially the form provided on the AMTSO website, which shall state that the Participant has complied with all requirements in Section 7.1, including any exceptions.

7.5. Vendors who do not notify the Tester of their intention to be a Voluntary Participant, or who do not comply with the requirements in Section 7.1, are not considered to be Voluntary Participants, and have no Voluntary Participant rights as defined here and in Section 9.

7.6. A Voluntary Participant may cease complying with the requirements in Section 7.1 at any time prior to the completion of the testing process, and thus is no longer a Voluntary Participant.

8. Behavior During a Test

8.1. Participant Behavior During a Test

8.1.1. All Participants in a test are prohibited from revising their Product while a test is knowingly being conducted with the “specific intent” of impacting the test results.

8.1.1.1. *Informative Reference.* “Specific intent” refers to an intentional plan or action by the Participant to impact the performance or results of testing such Participant’s Product, or the performance or results of any other Participant’s Product. Some examples include:

- When a feature is added for testing purposes only and not made commercially available.
- Features that only manifest themselves in tests and not in real-world scenarios that would be encountered by customers
- Features tuned to apply to known testing environments

8.1.1.2. *Informative Reference*. This Standard does not prohibit any general improvements meant for the end user, such as standard Cloud, feature, or signature updates. If any significant general improvements are made to any Products while a test is knowingly being conducted, information Vendor feels is relevant should be disclosed to the Tester.

8.1.2. Vendors and Testers shall keep each other informed of any changes to how Products operate and evidence is captured which may affect the running of ongoing tests or handling feedback. Significant changes include areas such as (i) logging format, (ii) the style and position of prompts or pop-ups, (iii) default configurations; and (iv) system requirements.

8.1.2.1. *Informative Reference.* As per the AMTSO Guidelines to Facilitating Testability, AMTSO strongly encourages open and timely communications between Testers and Vendors, particularly on issues which may affect how tests are run.

8.2. Tester Behavior During a Test.

8.2.1. Testers shall test all Participants' Products included in any Test Fairly and equally, regardless of whether the Test was commissioned and who commissioned the Test.

8.2.1.1. *Informative Reference.* Offering an advanced look at sample sets due to be used in Tests to some but not all Participants prior to testing is unfair.

8.2.1.2. *Informative Reference.* Test results containing misconfigured Products or disabled features, not agreed to in the Test Plan, is unfair.

8.2.1.3. *Informative Reference.* Not allowing Products to update to their latest available version is unfair.

8.2.2. Testers shall configure the tested Products for logging, and retain logs of material testing procedures for verifications and disputes until all disputes are completed.

8.2.2.1. *Informative Reference*. AMTSO Best Practices for Dynamic Testing. In dynamic tests, the behavior of Malware is crucial to how the Products perform, therefore, it is important for the Tester to have adequate logging and auditing of how the test proceeds. At the very least, this should cover: (i) the actions the Malware takes on the infected/compromised machine; (ii) modifications made to files, registry, and system areas; and (iii) traces of network activity.

8.2.2.2. *Informative Reference*. Please refer to AMTSO Guidelines on Facilitating Testability, Section 2, Logging, for a full description of details recommended to be included in logs, including: (i) an event occurred; (ii) time of event; (iii) a unique event ID or reference; (iv) event category or description; (v) source or originator of the event; (vi) threat id/Classification; (vii) actions taken; (viii) time taken between event and response/action. Additional examples of product-related content for logging: (i) initialization time; (ii) update time/version; (iii) version information.

8.2.3. If significant anomalous issues are detected during a Test run, the Tester shall attempt to contact the Participant to debug the situation, rather than simply stating that the Product is defective.

8.2.3.1. *Informative Reference.* This Standard is intended to prevent a Tester from ignoring an obviously flawed configuration or Test and encouraging the Tester to instead work with the Participant to ensure the Product is Fairly and accurately tested. A "significant anomalous issue" shall include an issue that a reasonable Tester would know to be notably inconsistent with the anticipated behavior of a Product.

8.2.4. After completion of a test run, the Tester shall notify all Participants in the Test, and is encouraged to provide initial results to each Participant with an appropriate amount of time reserved for feedback, dynamically based on the sample set size.

8.2.4.1. *Informative Reference*: A test run is considered complete when all tests have been performed and results collated and processed. Further retesting may be required as a result of later analysis or disputes.

8.2.4.2. *Informative Reference:* AMTSO Guidelines on Facilitating Testability. Testers are encouraged to provide Vendors taking part in their Tests with adequate information to diagnose and, ideally, to rectify any problems reported in tests – for example, failure to detect or block attacks.

9. Behavior After Completion of a Test.

9.1. Participant Behavior After a Test

9.1.1. Voluntary Participants shall have the right to audit their Product configuration.

9.1.1.1. *Informative Reference*: The audit of the Product configuration may be through reviewing relevant portions of associated logs for Participants who have human-readable (unencrypted) logs and have instructed the Tester how to enable logging.

9.1.1.2. *Informative Reference*: AMTSO encourages Testers to provide Vendors with access to the testing environment to validate configuration.

9.1.1.3. *Informative Reference*: AMTSO encourages Vendors to provide Testers with tools that would help validate configuration.

9.1.2. Test Commentary

9.1.2.1. Voluntary Participants shall have the right to attach Commentary regarding the Test and their specific Product's results in a meaningful way.

9.1.2.2. Participants other than Voluntary Participants may attach Commentary to the Test solely with regard to the specific reason(s) that such Vendor is not participating in the Test as a Voluntary Participant.

9.1.2.2.1. *Informative Reference*: Commentary on the Test Plan and reasons for not adopting Voluntary Participant status will be solicited at the Test commencement stage and no later adjustments will be accepted. Commentary should provide enough information for readers to understand the Participant's opinions clearly. AMTSO may review any Commentary for clarity and may suggest edits to the submitting party prior to publication.

9.1.2.3. AMTSO may attach Commentary regarding the Test's adherence to AMTSO's Testing Best Practices and Guidelines, and to the Test's own Test Plan.

9.1.2.3.1. *Informative Reference*: If a material failure to follow the Test Plan or established AMTSO Best Practices is alleged, AMTSO will review feedback from **all** Participants, and the Tester, and may choose to publish any details of this investigation as part of the Commentary.

9.1.2.4. Testers shall have the right to have a single response to each Vendor- and AMTSO-originated attached Commentary.

9.1.2.5. Commentary shall be included with the Test via hyperlink or otherwise in reference to the AMTSO website, which shall include the name of the Test, the Test results (which may be behind a paywall or otherwise restricted), and the Commentary.

9.1.2.6. AMTSO shall monitor and moderate all Commentary provided in this regard.

9.1.3. All Participants shall comply with AMTSO deadlines on Commentary submission, which

will be found on the AMTSO website.

9.1.3.1. *Informative Reference*: Any submissions received outside the appropriate timeframes will not be accepted as official Commentary, however AMTSO may choose to review or investigate any claims made in such submissions.

9.2. Tester Behavior After a Test

9.2.1. Testers shall present a Public Test's results in a way that is clear and understandable to prevent the results from being deceptive, unfair, or misleading.

9.2.1.1. *Informative Reference.* Any parties publicly using the Test results are encouraged to follow the publishing policy provided by the Tester as well as basic laws of advertising[2] and for use of endorsements, in that: (1) the claims must be truthful and not misleading; (2) there must be evidence to back up claims, and (3) the claims cannot be unfair.

9.2.2. Upon request and as soon as possible after the test run is completed, Testers shall provide individual Product logs to each Voluntary Participant whose Product provides human-readable (unencrypted) logs and has instructed the Tester how to enable logging.

9.2.2.1. Testers are not required to provide Tester-confidential information or certain personally identifiable information (PII). Any modifications to the logs must be denoted with a statement that it was done to protect confidential Tester intellectual property and PII.

9.2.2.1.1. *Informative Reference*. Even in cases where a Tester claims the sample or test case is Tester-confidential, the Tester must provide enough information so an experienced Vendor can validate how their Product performed and remediate any shortcomings in their Product. The Vendor defines how much information is sufficient for these purposes.

9.2.3. *Informative Reference.* Including results for uncompleted tests without clear notation in the details and the summary Test results is unfair.

9.2.4. The publicly released final Test results shall include:

9.2.4.1. A "usage statement" which covers this Standard.

9.2.4.2. Detailed information on the specific Products included in the Tests, including version details.

9.2.4.2.1. *Informative Reference*. Testers are encouraged to disclose which Participants requested to be excluded from the Test yet were included.

9.2.4.3. Potential material conflicts of interest by Participants and the Tester, or other commissioning parties, with regard to the particular Test.

9.2.4.3.1. *Informative Reference.* AMTSO encourages disclosure when test cases

[2] See, for example, the FTC Guides Concerning Use of Endorsements and Testimonials in Advertising.

and samples are provided by or selected by the commissioning party.

9.2.4.4. Other information that would be relevant to assess the Fairness of the Test.

9.2.4.4.1. *Informative Reference*: If a Tester has knowledge of a Participant's prior exposure to samples used in the test, whether because the Tester pre-notified certain Participants or otherwise, this would be relevant.

9.2.4.5. Any relevant non-confidential disclosures from Voluntary Participants

9.2.4.6. How the Test was (or will be) funded.

9.2.4.7. Other services that the Tester may offer that could have been accessed or consumed by a Vendor.

9.2.4.8. A reference to the Test Plan.

9.2.4.9. Data regarding the tests run, including date and time ranges, in a standard format so the results are clear and can be easily understood.

9.2.4.9.1. *Informative Reference*: Testers are not required to detail specific dates and times when individual test cases were performed, but should provide some information on the timing of major Test components, with particular reference to any differences between the timing of individual participants – for example, "tests were not run in parallel, but all products were exposed to each threat within a two-hour window".

9.2.4.10. A detailed test methodology

9.2.4.10.1. *Informative Reference:* The Test methodology should not require the Tester to release Tester-confidential information, but it should be detailed enough that an experienced Tester would have enough information to perform a similar test to validate the results.

9.2.4.11. Clear parameters on how Test results can be used.

9.2.4.11.1. *Informative Reference*: Testers should define how their results can be republished, with particular reference to republishing edited or summarized results. For example, Testers may want to require that anyone sharing excerpts of results must link back to the source.

9.2.4.12. Specific scores/certifications and any clarifying statements of statistical relevance.

9.2.4.12.1. *Informative Reference*: It is considered statistically relevant if some but not all Participants reviewed configurations or disputed samples. This disparity needs to be noted, along with the identification of those Participants, in clear connection to any specific scores/certifications, and in any comparative tables, charts, or graphs that contain disparate Participants, using these guidelines:

1) If the services were offered free of charge and not taken, the notation can be referential, such as an asterisk leading to a footnote or the Test results.

2) Otherwise the notation must be clear and explicit, including statements like "Some vendors were excluded from feedback processes," or "All vendors were invited, but some vendors declined to pay the feedback participation fee."

9.2.4.13. A hyperlink to the AMTSO website for readers to obtain "Additional Information" about each Public Test.

9.2.4.13.1. *Informative Reference.* This Standard allows critical additional information from both the Tester and Participants to remain accessible, even if included separately from the results.

9.2.4.13.2. To ensure effectiveness of this Standard, Tester must ensure the hyperlink: (1) is obvious; (2) appropriately shows the importance, nature, and relevance of the information it leads to; (3) is placed close to the relevant information that it is qualifying to ensure that it is noticeable, and significant scrolling is not necessary; (4) takes the end user directly to the disclosure on the click-through page.

9.2.4.13.3. Testers may choose to assess the effectiveness of the hyperlink by monitoring click-through rates and other information about end-user usage and make changes accordingly.

9.2.4.14. A statement of how the Products and their licenses were acquired.

9.2.5. Tester shall provide AMTSO with appropriate data to run the compliance confirmation process that is not otherwise included in the publicly released final Test results, including the Test Plan, Test results, and commentary.

9.2.6. Tester shall provide AMTSO with a complete and executed Tester Attestation, in substantially the form provided on the AMTSO website, which shall state that the Tester has complied with this Standard, as required for confirmation of compliance of the Test.

9.2.7. Tester shall notify AMTSO about the discovered material misuse of any Test results, and should respond to the alleged abuser, as appropriate.

9.2.8. Tester shall make timely amendment to any Test results that are still within any "dispute period" as necessary, based on material new information or the resolution of disputes.

9.2.9. Tester shall ensure that any party with rights to any Test results shall adhere to the contractual requirements of such Test, if applicable, and AMTSO guidelines regarding publication of the Test results, as set forth above.

10. AMTSO Requirements

As an organization, AMTSO has agreed to undertake certain obligations to help drive this Standard and a Test compliance program. Thus, AMTSO has agreed that it shall:

10.1. Develop and maintain testing protocol standard, which shall include regular review and updating of this Standard, as appropriate and necessary.

10.2. Host a repository for all Vendor and Tester contact information, voluntarily provided and updateable by each party.

10.3. Host a site where Testers can post Test Plans for Public Tests, and link back to the Tester's site for each Test.

10.4. Provide notice to AMTSO Members and others regarding the posting of any open Test Plan.

10.5. Complete the compliance confirmation process for submitted Tests in a timely manner.

10.6. Host publicly accessible webpages listing all Tests that successfully pass AMTSO's compliance confirmation process. The page will include the Test Plan, Participants and their status, the Tester, and Participant commentary.

10.7. Provide support and resolution to Testers and Vendors with regard to questions regarding compliance with this Standard.

10.8. Respond in a timely manner to inquiries regarding any Vendor, Tester or accredited Test, including regarding allegations of improper behavior.

10.9. Publicly defend a properly accredited Test when accusations of improper behavior are settled.

10.10. Help facilitate arbitration between Vendors and Testers, as appropriate and as necessary.

10.11. Help resolve issues regarding improper use of test results.

10.12. Serve as an advocate for the rights of Testers to have access to and test all Anti-Malware Products.

10.13. Host a public test page for all tests submitted for confirmation of compliance, the Test Plan, and the final disposition of compliance review.

10.14. Host a public page attempting to show the relevant observed holidays by country.

10.15. Promote the value of accredited tests that follow this Standard.

10.16. Make efforts to verify Vendors and contacts for inclusion onto the AMTSO website.

This document was adopted by AMTSO on (2017-12-05 APPROVED DRAFT)