Keywords: anti-malware; protocol; standard; test

AMTSO 1:2018
October 24, 2018

Version 1.1

Testing Protocol
Standard for the Testing of
Anti-Malware Solutions

Sponsored by:

The Anti-Malware Testing Standards Organization, Inc.
AMTSO Member Approval Date 2018-10-24
AMTSO Board Approval Date 2018-10-24

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 Working Group via email to: standards@amtso.org.

AMTSO Standards Working Group

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

Name of Representative	**Affiliation**
Brad Albrecht	*CrowdStrike*
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*
Samaresh Nair	*Palo Alto Networks*
Samir Mody	*K7 Computing*
Scott Jeffreys	*AMTSO*
Simon Edwards	*SE Labs*

Former SWG members
(contributing to previous versions)

Name of Representative	**Affiliation**
Andreas Clementi	*AV-Comparatives*
Bhaarath Venkateswaran	*NSS Labs*
Chad Skipper	*Cylance*
Scott Marcks	*Cylance*

Table of Contents

Testing Protocol Standard 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 participation by Vendors
- Establishing methods for Vendor notification
- Supporting disclosure of prior access to Test samples, sample provenance, and sample Curation strategy
- 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 Test Subject Vendors, 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 terms "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 Test Subject Vendor on a Test Plan or the Test results, as submitted by Test Subject Vendors 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.** An optional process in which Testers provide Test Subject Vendors 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. **Feedback Process.** See Dispute Process.

2.2.14. **Golden Sample.** A version of a Product specifically designed to be as good as possible, or to perform particularly well in a specific type of test, and not distributed to the broader user base.

2.2.15. **Included Product.** A Test Subject, the Vendor of which has not chosen to adopt Participant status.

2.2.16. **Included Vendor.** The Vendor of an Included Product, which has not chosen to adopt Participant status.

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

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

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

2.2.20. **Participant.** The Vendor of a Test Subject, which has chosen to adopt Participant status and engage with the Tester, and has complied with the requirements to maintain such status as set forth in Section 7 below.

2.2.21. **Participant Product.** A Test Subject, the Vendor of which has chosen to adopt Participant status and engage with the Tester, and has complied with the requirements to maintain such status as set forth in Section 7 below.

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

2.2.23. **Product.** An Anti-Malware solution. All Products have the potential to be tested. When a Tester decides to place a Product in a Test, that Product becomes a Test Subject.

2.2.24. **Public Test.** An Anti-Malware Test where the Tester or its Test Subject Vendors intend to publish or publicly reference its existence or its results.

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

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

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

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

2.2.29. **Test Subject.** A Product, which a Tester has indicated they plan to include in a Test.

2.2.30. **Tester.** An individual or entity that conducts Tests on Anti-Malware Products to establish functionality, effectiveness, comparative results, compliance, or other determinations. In cases where a Test is commissioned by a third party, the commissioning party may, with the agreement of the test lab they are contracting, choose to take the role of Tester under this Standard. In such circumstances the test lab, or other individual or entity performing the work, acts as a sub-contractor.

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

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 a Test Subject 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, Vendors or third parties 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 Test Subject Vendors.

4.1.1. *Informative Reference*: Sending notification and the Test Plan directly to the potential Test Subject Vendors through use of contact information contained in the AMTSO Contact List system described in Section 3, or through public notification of the Test Plan in compliance with Section 5 herein, is considered notification. If the Tester does not wish to make the Test Plan publicly available at the notification stage, this should be noted

when providing the Test Plan to AMTSO. All Test Plans will be posted on the "Compliance Summary" page on publication of each Test.

4.1.2. *Informative Reference*: Testers should retain information on the notification process (who was contacted, how and when) to assist with verification.

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 Test Subject Vendor 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 Test Subject Vendors through use of contact information on the AMTSO Contact List shall provide notification to all potential Test Subject Vendors at approximately the same time. This is to ensure that no potential Test Subject Vendors are provided significant advance notice over other potential Test Subject Vendors, 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 Test Subject Vendors 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 Test Subject Vendors 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 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 Test Subjects will be tested against.

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

6.1.4.1. *Informative Reference:* If the Tester is unsure of the exact Commencement Date, or wishes to avoid providing a specific date, a range of dates of up to three calendar months may be provided. For the purposes of notification timings, the first date of any range shall be treated as the Commencement Date.

6.1.5. If the Test Plan requires Test Subject Vendors to perform any specific actions, 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. *Informative Reference:* Test environment details should include at least expected operating system versions and patch levels, and policy of using virtualized or "bare metal" hardware.

6.1.6.2. *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 types or versions, configurations to be applied, and which functionality of the Products will be tested.

6.1.7.1. *Informative Reference:* At the Test Plan stage exact version details may not be available or predictable, but Testers should define their policy as to which version will be used, for example "most recent major release" or "2020 edition".

6.1.7.2. *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 Best Practices for Testing in-the-Cloud Security Products.

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

6.1.9. Details of what information and evidence will be provided to Test Subject Vendors prior to publication, whether feedback and Dispute services will be offered, and, where applicable, instructions on how the Test's results can be disputed.

6.1.9.1. *Informative Reference:* Testers may choose to offer preview of results and access to feedback and Dispute services only to Participants, or only to clients receiving additional paid consultancy services, at the Tester's discretion. A clear policy on such provisions should be defined in the Test Plan.

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

6.1.10.1. A Tester shall provide all Test Subject Vendors with the option to adopt Participant status, as set forth in Section 7. A Test may still comply with this Standard if only some, or none, of the Test Subject Vendors accept the option to adopt Participant status.

6.1.10.1.1. *Informative Reference:* AMTSO's desire is that any Test Subject Vendor should want to, and have the ability to, adopt Participant status.

6.1.10.2. A Tester shall not charge additional fees for Test Subject Vendors to adopt Participant status.

6.1.10.2.1. *Informative Reference:* AMTSO's goal with having Participant status is that in exchange for engaging with Testers and following disclosure requirements, Participants have additional rights to audit their Product's configuration, and to provide Commentary on Test results.

6.1.10.2.2. *Informative Reference:* If a Test has an entry fee and a Vendor declines to pay this fee, they are not a Test Subject Vendor, are not part of the Test and have no right, or reason, to adopt Participant status. If a Product is placed into a Test by the Tester, whether free of charge or for an entry fee, that Product becomes a Test Subject and its Test Subject Vendor has the right to adopt Participant status, and acquire the associated rights and obligations, at no additional cost.

6.1.10.2.3. *Informative Reference:* If a Tester chooses to offer other services such as Disputes, these may be offered to all Test Subject Vendors, or to Participants only, and may be offered freely or at a cost, at the Tester's discretion. Testers may also choose to offer access to configuration audit and Product logs, free of charge or at a cost, to "Included" Test Subject Vendors who have not chosen to adopt Participant status. A policy on how such services will be offered should be included in the Test Plan.

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 Test Subject Vendors to understand why the samples are considered relevant, but not so much information as to be administratively burdensome for the Tester or allow Test Subject Vendors to unfairly influence the Test execution or results.

6.1.11.2. *Informative Reference:* The Tester should utilize a Curation approach that does not allow any Test Subject Vendor to unfairly influence the Test execution or results.

6.1.12. A clear description of how samples will be Curated, and whether vendor input will be sought to confirm accurate Curation (see also 6.1.9 above).

6.1.12.1. *Informative Reference*: If Testers choose to limit Vendor involvement in sample Curation to only include Participants, then all Participants must be given equal opportunities to take part in such Curation and feedback processes for all their respective Products.

6.1.12.2. *Informative Reference*: Testers should select only samples and Test Cases which can be provided to Test Subject Vendors for independent validation, or for which all Test Subject Vendors can be provided with both adequate evidence of accurate Curation, and adequate information to enable the Test Subject Vendors to remediate any shortcomings in their Product.

6.1.12.3. *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 Test Subject Vendors to unfairly influence their Test results.

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

6.1.12.5. *Informative Reference:* If a Test covers Test Subjects which were identified by their 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:* 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.

6.2.2. *Informative Reference:* Testers are encouraged to include a policy on how Test Subjects may be dropped from a Test or omitted from the final Test Report. This policy should include definitions and timeframes for when it will be acceptable for Test Subjects to be withdrawn from a Test by their Vendors, and for the circumstances under which a Tester would decide to drop a Test Subject. It should also set expectations around public announcement of a dropped or omitted Test Subject. In the event that the parties involved disagree on the use of such policies, AMTSO will offer arbitration to help resolve differences.

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

- Disclosure for each Test Subject 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 Test Subject Vendors 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 Participants, or changes to the Commencement Date of a Test moving that date outside the notification requirements in Section 4.3.

7. Participants

In response to the Test Plan, all Test Subject Vendors may choose to adopt Participant status 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. All Participants 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." [1] 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.

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

7.1.5.1. *Informative Reference:* A Tester may rely on the assertion or omission of a Participant regarding the use of any third-party intellectual property included in the Product to be tested. If a Vendor claims a component is properly licensed, the Tester has no duty to investigate further.

7.2. In completing the disclosure requirements, a 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 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 of this provision is to encourage open and honest disclosure by the Participant to improve the potential for accurate Test results.

7.3. 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.

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. Participants shall provide the Tester with a complete and executed 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 Participant, or who do not comply with the requirements in Section 7.1, are not considered to be Participants, and have no Participant rights as defined here and in Section 9.

7.5.1. *Informative Reference:* Testers may, at their discretion, extend or adjust any deadlines set on provision of attestations and decisions on adopting Participant status, to accommodate Vendors unable to meet such deadlines. Any such policy must be applied equally to all Test Subjects.

7.5.2. *Informative Reference:* Vendors are strongly encouraged to respond to notifications

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

issued by Testers, regardless of their intent to adopt Participant status.

7.6. A Participant may cease complying with the requirements in Section 7.1 and 7.3 at any time prior to the completion of the testing process, and may thus lose Participant status.

7.6.1. *Informative Reference:* If a Tester considers a Participant to have forfeited their Participant status through failure to meet the requirements of Section 7.1 or Section 7.3, the Tester should inform AMTSO and the Participant of this decision, along with the grounds on which it was made.

7.6.2. *Informative Reference:* Testers may, at their discretion, accept minor infractions of these requirements and allow Test Subject Vendors to maintain Participant status. Any such policy must be applied equally to all Test Subjects.

8. Behavior During a Test

8.1. Vendor Behavior During a Test

8.1.1. All Test Subject Vendors are prohibited from revising their Product while a Test is knowingly being conducted with the "specific intent" of impacting the Test execution or results.

8.1.1.1. *Informative Reference:* "Specific intent" refers to an intentional plan or action by the Test Subject Vendor to impact the performance or results of testing such Test Subject, or the performance or results of any other Test Subject. 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, any information a Vendor feels is relevant should be disclosed to the Tester.

8.1.2. Test Subject 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 on Facilitating Testability, AMTSO strongly encourages open and timely communications between Testers and Vendors, particularly on issues which may affect tests and/or testing processes.

8.1.2.2. *Informative Reference:* In the event that a Vendor observes or is made aware of any

issue in the Test design or Test environment which could materially impact the execution or results of the Test, they are strongly encouraged to provide the Tester with adequate information to diagnose and rectify the issue, and to respond to requests for further information or assistance promptly.

8.2. Tester Behavior During a Test

8.2.1. Testers shall test all Test Subjects Fairly and equally in any Test, 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 Test Subject Vendors prior to testing is unfair.

8.2.1.2. *Informative Reference:* Testing using samples sourced from common industry or commercial feeds, which may be accessible to some Test Subject Vendors but not others, should be disclosed.

8.2.1.3. *Informative Reference:* Test results obtained using misconfigured Test Subjects or disabled features, not agreed to in the Test Plan, is unfair.

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

8.2.2. Where appropriate and possible without imposing undue or unnatural influence on the Test results, Testers shall configure Test Subjects for logging, and shall retain all available 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. Participants shall have the right to audit their Product configuration on request.

8.2.3.1. *Informative Reference:* The audit of the Test Subject 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. Screenshots, videos or other methods may also be acceptable as evidence of

appropriate configuration.

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

8.2.3.3. *Informative Reference:* AMTSO encourages Vendors to provide Testers with tools that would help validate configuration, and to include detailed, human-readable logging facilities in their Products.

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

8.2.4.1. *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 Test Subject Vendor 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. For example, a minor variation in the level of protection provided, or a normal software bug, is not considered anomalous; a drop in detection from 90% to 0% from one month to the next, or the complete failure of a piece of software to install or launch, should be considered anomalous.

8.2.5. After completion of a Test run, the Tester is encouraged to provide initial results to each Test Subject Vendor with an appropriate amount of time reserved for feedback, dynamically based on the sample set size.

8.2.5.1. *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.

8.2.5.2. *Informative Reference*: Testers may choose to provide each Test Subject Vendor with a preview of only the results for their own Product, or may share a preview of the full set of Test data, at the Tester's discretion.

8.2.5.3. *Informative Reference:* Testers may choose to offer a preview of results and access to feedback and disputes services only to Participants, or only to clients receiving additional paid consultancy services, at the Tester's discretion and following the policy defined in the Test Plan.

8.2.5.4. *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. Vendor Behavior After a Test

9.1.1. Test Commentary

9.1.1.1. Participants shall have the right to provide Commentary regarding the Test and their specific Product's results in a meaningful way for publication on the AMTSO website.

9.1.1.2. "Included" Test Subject Vendors may attach Commentary to the Test solely with regard to the specific reason(s) that such Vendor has not chosen to adopt Participant status.

9.1.1.2.1. *Informative Reference*: Commentary on the Test Plan and reasons for not adopting 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 Test Subject Vendor's opinions clearly. AMTSO may review any Commentary for clarity and may suggest edits to the submitting party prior to publication.

9.1.1.3. 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.

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

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

9.1.1.5. Commentary shall be referenced from the Test report via hyperlink or otherwise leading to the relevant "Compliance Summary" page on the AMTSO website, which shall include the name of the Test, reference to the Test results (which may be behind a paywall or otherwise restricted), and the Commentary.

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

9.1.1.7. *Informative Reference*: Vendors are encouraged to link to the "Compliance Summary" page for any Test or Test results they reference publicly. Testers may wish to include a requirement for this is their agreements for Testing or use of results.

9.1.2. All Test Subject Vendors shall comply with AMTSO deadlines on Commentary submission, as communicated by AMTSO or the Tester when issuing requests for Commentary.

9.1.2.1. *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. On completion of a Test, the Tester should retain any evidence on which their results and conclusions are based for later reference. Testers are encouraged to make such evidence available to Test Subject Vendors on request, to enable them to review and confirm the Tester's conclusions, or to flag up any potential errors.

9.2.2.1. *Informative Reference:* Useful evidence may include logs generated by Test Subject Products, at client or server side; logs produced by the Tester's internal tools; screenshots and videos; packet captures, replay systems or actual samples used in testing; or any other materials from which the Tester has drawn conclusions. In cases where large amounts of evidence are requested, providing a subset of the evidence captured may be appropriate to allow a Vendor to diagnose an issue. Testers should define a policy on what evidence will be made available in the Test Plan.

9.2.2.2. *Informative Reference:* Testers are not required to provide Tester-confidential information or personally identifiable information (PII). Any modifications to the logs should be denoted with a statement that it was done to protect confidential Tester intellectual property and/or PII.

9.2.2.3. *Informative Reference:* In cases where a Tester claims a sample, test case or other item of evidence is Tester-confidential, the Tester should provide sufficient information to enable an experienced Vendor to validate how their Product performed, and to remediate any shortcomings in their Product. Testers are encouraged to respect Test Subject Vendors' definition of how much information is sufficient to allow them to fully understand and address any issues. In cases where agreement cannot be reached, AMTSO shall offer arbitration.

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 Test Subject Products, including version details.

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

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

9.2.4.3. Potential material conflicts of interest by Test Subject Vendors 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 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 Test Subject's prior exposure to samples used in the test, whether because the Tester pre-notified certain Test Subject Vendors or otherwise, this would be relevant.

9.2.4.5. Any relevant non-confidential disclosures from Participants

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

9.2.4.6.1. *Informative Reference:* Funding models should match those proposed in the Test Plan, and any divergence from the Test Plan should be noted.

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 any limitations were imposed on access to Dispute processes AND if some but not all Test Subject Vendors took part in these processes. This disparity needs to be noted, along with the identification of those Test Subjects, in clear connection to any specific scores/certifications, and in any comparative tables, charts, or graphs that contain disparate Test Subjects, using these guidelines:

- If the services were offered without limitation and not taken, the notation can be referential, such as an asterisk leading to a footnote or the Test results.
- 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 take part."

9.2.4.13. A URL or hyperlink to the AMTSO website for readers to find the "Compliance Summary" for each Public Test.

9.2.4.13.1. *Informative Reference:* This Standard allows critical additional information from both the Tester and Test Subject Vendors 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 URL or 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 "Compliance Summary" page.

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. Testers and Vendors shall notify AMTSO about the discovered material misuse of any Test results, and should respond to the alleged abuser or request that AMTSO do so, 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 Test which complies with this Standard when accusations of improper behavior are brought.

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 "Compliance Summary" page for all Tests submitted for confirmation of compliance, including the Test Plan, Commentary, and the final disposition of compliance review.

10.13.1. *Informative Reference:* If a Test is submitted to AMTSO for confirmation of compliance, it can be withdrawn from the process by the tester at any time. If withdrawal is requested before any additional artefacts are gathered by AMTSO, such as initial "Phase 1"

Commentary, or if the test is ultimately not published, the Test notification, Test Plan and other details shall be removed from the AMTSO website. If withdrawal is requested later and the Test is published, AMTSO shall retain the notification details, Test Plan and any Commentary for reference.

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 as a Final Standard by AMTSO on 2018-10-24