DoD Annex
for the
Web Browser
Protection Profile

Version 1, Release 3

5 May 2014

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

A National Information Assurance Program (NIAP) approved Protection Profile (PP) includes requirements to ensure particular functionality is present and can be tested in a commercial product. It is possible there will be cases in which selections meet PP requirements but do not meet DoD-mandated specific values.

In accordance with the NIAP *Protection Profile for Web Browsers* (version 1.0, dated 31 March 2014), selections, assignments, and objective requirements may be included in the NIAP Common Criteria Security Target (ST) such that the product still conforms to the PP. This document addresses the DoD specificity needed for web browsers to be used within the DoD. As such, any vendor that wishes to be certified for DoD use must indicate that they are claiming compliance with both the PP and the DoD Annex, and include the specified selections, assignments, and requirements in the ST upon initiation of a NIAP evaluation.

While a NIAP certificate can be awarded as long as the product meets all requirements in the PP, for use in the DoD it is also mandated that the product address all requirements listed in this DoD Annex.

1.2 Scope

The additional information in this document is applicable to all DoD-administered systems and all systems connected to DoD networks.

1.3 Relationship to STIGs

This DoD Annex for Web Browser Protection Profile (WBPP) addresses the DoD specificity to the NIST SP 800-53 controls identified in the WBPP. As a result, the Annex, in conjunction with the PP, serves as a single specification within the DoD for security of Web Browsers.

The publication of the Annex does not eliminate the DoD need for a product-specific Security Technical Implementation Guide (STIG); however, the results of the Common Criteria evaluation will be used to formulate a STIG. The benefit of this approach is that at the conclusion of a successful NIAP evaluation, a vendor's product will be certified as meeting the requisite NIST SP 800-53 controls, and much of the information needed for a STIG will be gathered from Common Criteria artifacts. Upon publication of a STIG, the product may be used within the DoD. STIGs will continue to be published in XCCDF format along with automation where applicable for assessment, as well as baseline configuration guidance for DoD.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

2. DOD-MANDATED SPECIFIC VALUES

Convention: Underlined text indicates assignments to be included in the WBPP-conformant Security Target (ST) that are mandated in the DoD environment. Strikethrough text indicates a selection that should be absent from the ST or capable of being disabled via Target of Evaluation (TOE) configuration.

2.1 DoD Assignments and Selections

The following assignments and selections from Security Functional Requirements are mandated for the DoD:

SFR ID	DoD Selections and Assignments
FDP_SBX_EXT.1.1	[selection: [assignment: methods by which the principle of least privilege is implement for rendering processes], ~~in no other ways~~].
FDP_TRK_EXT.1.1	[selection: ~~web sites accessed, geo-location information, system configuration, system status, error conditions, crash conditions,~~ [assignment: no tracking information]]
FPT_MCD_EXT.1.1	[selection: ActiveX, Flash, Java, JavaScript, VBScript, MS-DOS batch scripts, UNIX shell scripts, binary executables, Shockwave movies, Java mobile code]
FPT_MCD_EXT.1.3	[selection: ActiveX, Flash, Java, JavaScript, [assignment: VBScript when executed with the Windows Scripting Host (WSH)]]
FIA_X509_EXT.1.1	[selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759] Note: An ST that includes a CRL selection is acceptable provided that it also selects OSCP and provides a management functionality to require OSCP over CRL.
FIA_X509_EXT.2.1	[selection: code signing for extension installation, code signing for plug-in installation~~, no additional uses~~]
FIA_X509_EXT.2.2	[selection: ~~allow the administrator to choose whether to accept the certificate in these cases , accept the certificate~~, not accept the certificate]
FPT_TUD_EXT.1.1	[selection: extension, plug-in, ~~no other add-~~

	~~on~~]
FPT_TUD_EXT.1.2	[selection: extension, plug-in, ~~no other add-on~~]
FPT_TUD_EXT.1.3	[selection: extension, plug-in, ~~no other add-on~~]
FPT_TUD_EXT.1.4	[selection: extension, plug-in, ~~no other add-on~~]

2.2 Objective/Optional Functions Mandated for DoD

The following objective and optional Security Functional Requirements are mandated for the DoD:

SFR ID	Application Notes
FAU_GEN.1.1	The audit logs must include a history of: • Websites visited • Files downloaded from remote systems
FAU_GEN.1.2	Application notes: • The type of event includes the protocol used when the event was generated (HTTP, HTTPS, FTP, etc.). • The subject identity includes the complete URL of the site accessed when the event was generated.

2.3 DoD-Mandated Configuration

The following configuration values must be supported in DoD field implementations of the TOE:

SFR ID	DoD Field Configuration
FIA_X509_EXT.1	The TOE must be able to access DoD root and intermediate certificates either through configuration of the TOE or its underlying platform. DoD public key certificates must be obtained from an approved service provider.
FMT_MOF.1.1	Any selection listed for FMT_MOF.1.1 in Section 2.1 must be activated in implementation to the extent it is configurable.
FMT_SMF.1.1 Function 4	Disable websites accessed, geo-location information, system configuration, system status, error conditions, and crash conditions.
FMT_SMF.1.1 Function 5c	Delete passwords and other sensitive data.

FMT_SMF.1.1 Function 6	Unsigned ActiveX, Java scripts, and VBScript when executed within the Windows Scripting Host (WSH) must be blocked. Prompt the user before execution of signed ActiveX, and java scripts and VBScript when executed within the Windows Scripting Host (WSH). Signed Scrap objects (e.g., .shs and .shb files), MS-DOS scripts, UNIX scripts, binary executables, Shockwave movies, ActiveX, Java scripts, and VBScript must be blocked when obtained from an untrusted or unverified source.
FMT_SMF.1.1 Function 13	Disable the storage of sensitive information in persistent storage.
FMT_SMF.1.1 Function 14	Enable use of OCSP for obtaining the revocation status of an X.509 certificate.
FMT_SMF.1.1 Function 15	Disable interaction with the Graphics Processing Units (GPUs).
FMT_SMF.1.1 Function 16	Disable use of private browsing sessions.
FMT_SMF.1.1 Function 19	Disable establishment of a trusted channel if the TSF cannot establish a connection to determine the validity of a certificate.
FMT_SMF.1.1 Function 20	Disable ability for websites to register protocol handlers.