DoD ANNEX
FOR
APPLICATION SOFTWARE EXTENDED PACKAGE
FOR WEB BROWSERS

Version 1, Release 1

16 July 2015

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

1.1 Background

This Annex to the Application Software Extended Package for Web Browsers (version 2.0, dated 16 June 2015) delineates Extended Package (EP) content that must be included in the Security Target (ST) for the Target of Evaluation (TOE) to be fully compliant with DoD cybersecurity policies pertaining to information systems. This content includes DoD-mandated EP selections and assignments and PP Security Functional Requirements (SFRs) listed as optional or objective in the PP but which are mandated in DoD.

Deficiencies of the TOE with respect to the DoD Annex will be reported as appropriate under the Risk Management Framework for DoD Information Technology (DoD Instruction 8510.01). DoD may determine that a TOE that does not conform to this Annex may pose an unacceptable risk to DoD. Accordingly, any vendor seeking authorization for use of its product within DoD should include the additional PP specificity described in this Annex in its ST.

The Extended Package for Web Browsers, in conjunction with this Annex, addresses the DoD-required cybersecurity controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Taken together, they supersede the DoD Mobile Device Management Security Requirements Guide.

1.2 Scope

The additional information in this document is applicable to all browsers connected to DoD networks.

1.3 Relationship to Security Technical Implementation Guides (STIGs)

A successful Common Criteria evaluation certifies the capabilities of the TOE but does not assure its subsequent secure operation. To address security concerns with the ongoing operation of the TOE in the field, a product-specific STIG is prepared in conjunction with the Common Criteria evaluation. The STIG lists the configuration requirements for DoD implementations of the TOE and is published in eXtensible Configuration Checklist Description Format (XCCDF) to facilitate automation where feasible.

This Annex contains the required DoD configuration of features implementing the Security Management (FMT) class of SFRs listed in the PP for Application Software. For each applicable FMT SFR, the STIG will discuss the vulnerability associated with non-compliance configuration and provide step-by-step, product-specific procedures for checking for compliant configurations and fixing non-compliant configurations.

In most cases, the ST will not cover all security-relevant configurable parameters available in the TOE. However, the STIG will include these whenever they impact the security posture of DoD information systems and networks. Accordingly, the DoD Annex only addresses a subset of the controls expected to be included in a STIG.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via email to: disa.stig_spt@mail.mil.

2. DOD-MANDATED SECURITY TARGET CONTENT

The following conventions are used to describe DoD-mandated ST content:

- If an EP SFR is not listed, there is no DoD-mandated selection or assignment for that SFR.
- For EP selections:
  - The presence of the selection indicates this is a DoD-mandated selection.
  - If a selection is not listed, then its inclusion or exclusion does not impact DoD compliance.
  - Underlined text indicates a selection.
  - *Italicized and underlined* text indicates an assignment within a selection.
  - ~~Strikethrough~~ text indicates that the ST author must exclude the selection.
- For EP assignments:
  - The DoD-mandated assignments are listed after the assignment parameter.
  - If an assignment value appears in ~~strikethrough~~ text, this indicates that the assignment must not include this value.
  - *Italicized* text indicates an assignment.

The Annex provides the minimum text necessary to disambiguate selections and assignments. Readers will need to view both the EP and the DoD Annex simultaneously to place the Annex information in context.

2.1 DoD-Mandated Assignments and Selections

DoD mandates the following EP SFR selections and assignments for SFRs in Section 4 of the PP for Application Software:

Table 2-1: EP SFR Selections

SFR	Selections, Assignments, and Application Notes
FDP_SBX_EXT.1.1	*through methods by which the principle of least privilege is implemented for rendering processes*
FDP_TRK_EXT.1.1	websites accessed, geolocation, browser history, browser preferences, browser statistics
FMT_MOF_EXT.1.1	*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.*

SFR	Selections, Assignments, and Application Notes
FPT_MCD_EXT.1.1	ActiveX, Flash, Java, *[assignment: other mobile code types supported by the browser]*
FPT_MCD_EXT.1.2	ActiveX, Flash, Java, *[assignment: other mobile code types supported by the browser]*

2.2 DoD-Mandated Optional, Selection-Based, and Objective SFRs

There are no optional or objective SFRs listed in the EP mandated by the DoD.

3. OTHER DOD MANDATES

3.1 Federal Information Processing Standard (FIPS) 140-2

Not included in this Annex.

3.2 Federal Information Processing Standard (FIPS) 201-2

The TOE is expected to interface with FIPS 201-2 compliant credentials (to include derived credentials as described in NIST Special Publication 800-157). The TOE may communicate with a peripheral device (e.g., a smart card reader) in order to interface with PIV credentials, or natively store derived credentials (whose protections are evaluated in the Protection Profile).

3.3 DoD-Mandated Configuration

The table below lists configuration values for product features implementing the EP Specification of Management Functions (FMT_SMF). The ST is not expected to include this configuration information, but it will be included in the product-specific STIG associated with the evaluated IT product. Non-binary configuration values are shown in *italics*.

Table 3-1: Configuration Values

FMT_MOF_EXT.1.1 Function	DoD Selections and Values
3	Enable
5	Disable
6	Delete passwords and other sensitive data.
7	Disable
10	Disable
12	Disable
16	Disable
17	Enable
21	Enable