DoD Annex
for
Protection Profile for Application Software v1.0

Version 1, Release 1

22 October 2014

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 FSO of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

1. INTRODUCTION

1.1 Background

This Annex to the *Protection Profile (PP) for Application Software* (Version 1.0, dated 22 October 2014) delineates PP 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 PP selections and assignments, and PP security functional requirements (SFRs) listed as optional or objective in the PP but which are mandated in the DoD. As stated in DoD Instruction 8500.01 "Cybersecurity," NIAP evaluation is expected for IA and IA-enabled products in accordance with CNSSP 11. Evaluation of applications without IA functionality is at the discretion of the Authorizing Official."

Any 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 that does not conform to this Annex may pose an unacceptable risk to the DoD. Accordingly, any vendor seeking authorization for use of its product within the DoD should include the additional PP specificity described in this Annex in its ST.

The APP SW PP, 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 Application Security Requirements Guide.

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 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 in the APP SW PP. 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. A STIG includes all security parameters under the control of the user or administrator, indicating secure values as appropriate. Additional configuration requirements for more-specialized applications may also be captured in DoD Annexes to Extended Packages of the APP SW PP.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via email to: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

2. DOD-MANDATED SECURITY TARGET CONTENT

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

- If a PP SFR is not listed, there is no DoD-mandated selection or assignment for that SFR.

- For PP 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.
  - Strikethrough text indicates that the ST author must exclude the selection.

- For PP 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.

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

2.1 DoD Assignments and Selections

DoD mandates the following PP SFR selections and assignments for SFRs in the main body of the PP:

Table 2-1: PP SFR Selections

SFR	Selections, Assignments, and Application Notes
FMT_SMF.1	*list of other management functions to be provided by the TSF* = deny all inbound UDP/TCP traffic except traffic on *[assignment: list of TCP/UDP ports]*. Application note: The mobile app must utilize ports or protocols in a manner consistent with DoD Ports and Protocols guidance, including the DoD Ports Protocols Services Management (PPSM) Category Assurance List (CAL). If it does so natively, this management functionality is not required. If it does not do so, then it must permit configuration to obtain a state consistent with the PPSM CAL.

2.2 DoD-mandated Selection and Objective Functions

There are no objective or optional Security Functional Requirements mandated for the DoD.

3. OTHER DOD MANDATES

3.1 Federal Information Processing Standard (FIPS) 140-2

Cryptographic modules supporting any SFR in the Cryptographic Support (FCS) class must be FIPS140-2 validated. While information concerning FIPS 140-2 validation should not be included in the ST, failure to obtain validation could preclude use of the TOE within DoD.

3.2 Federal Information Processing Standard (FIPS) 201-2

Where the TOE supports authentication to remote DoD servers, it is expected to interface with FIPS 201-2 compliant credentials (to include derived credentials as described in NIST 800-157) provided by the TOE platform. The TOE platform may connect to a peripheral (e.g., a smart card reader).

3.3 DoD-Mandated Configuration

The table below lists configuration values for product features implementing the PP 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

SFR	DoD Selections and Values
FMT_SMF.1.1	*[**assignment:** list of DoD-approved TCP/UDP ports included in the DoD Ports Protocols Services Management (PPSM) Category Assurance List (CAL)]*