AUSTRALIAN SIGNALS DIRECTORATE

MANDATORY REQUIREMENTS ADDENDUM

PROTECTION PROFILE FOR MOBILE DEVICE FUNDAMENTALS VERSION 1.1 DATED 12 FEB 2014

In accordance with the *Protection Profile for Mobile Device Fundamentals (Version 1.1 dated 12 Feb 2014)* the Objective Requirements listed below may be included in the Security Target (ST) such that the Target of Evaluation (TOE) is still conformant to this Protection Profile (PP).

These additional objective requirements must be included in a ST as a prerequisite to the TOE being considered for an Australian Signals Directorate (ASD) Cryptographic Evaluation (ACE). Only after the successful completion of the ACE will ASD consider certifying a device as suitable for the protection of Australian Government information at the PROTECTED level.

Users of the *Protection Profile for Mobile Device Fundamentals (Version 1.1 dated 12 Feb 2014)* must refer to the Application Notes and Assurance Activities listed under each Security Functional Requirement.

D.3. CLASS: USER DATA PROTECTION (FDP)

- D.3.1. ACCESS CONTROL (FDP_ACF)

FDP_ACF_EXT.1 EXTENDED: SECURITY ATTRIBUTE BASED ACCESS CONTROL

- **FDP_ACF_EXT.1.2**

- D.3.2. DATA-AT-REST PROTECTION (FDP_DAR)

FDP_DAR_EXT.2 SENSITIVE DATA ENCRYPTION

- **FDP_DAR_EXT.2.1**
- **FDP_DAR_EXT.2.2**
- **FDP_DAR_EXT.2.3**
- **FDP_DAR_EXT.2.4**

D.6. CLASS: PROTECTION OF THE TSF (FPT)

- D.6.1. ANTI-EXPLOITATION SERVICES (FPT_AEX)

FPT_AEX_EXT.1 EXTENDED: ANTI-EXPLOITATION SERVICES (ASLR)

- **FPT_AEX_EXT.1.3**
- **FPT_AEX_EXT.1.4**

FPT_AEX_EXT.2 EXTENDED: ANTI-EXPLOITATION SERVICES (MEMORY PAGE PERMISSIONS)

- **FPT_AEX_EXT.2.2**

ENTROPY REQUIREMENTS

Vendors must meet design documentation and data collection requirements of entropy sources as described in NIST special publication SP800-90B in order to enable validation testing.