Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

BROADCAST

APRIL 2014

EVALUATION PATHWAY FOR MOBILE DEVICES

Introduction

1. The purpose of this broadcast is to define the Australian Signals Directorates' (ASD) evaluation pathway for mobile devices for use within the Australian Government. It details the progressive steps towards certification of a mobile device in meeting the Information Security Manual's (ISM) requirements for ICT equipment containing PROTECTED information to be handled at an UNCLASSIFIED level.

2. ASD has previously endorsed Protection Profiles in several key technology-specific areas and has now endorsed the below Protection Profiles published by the United States' National Information Assurance Partnership (NIAP):

- Protection Profile for Mobile Device Fundamentals (MDFPP) v 1.0,
- Protection Profile for Mobile Device Fundamentals (MDFPP) v 1.1.

Evaluation Pathway

3. The following three phases outline the evaluation pathway.

Phase 1 – For a mobile device to be considered suitable for the protection of Australian Government information at the UNCLASSIFIED/DLM Level, in accordance with the ISM's "Government" system applicability indicator, it must successfully complete a Common Criteria evaluation against an ASD endorsed Protection Profile. It must also be operating in its evaluated configuration.

Phase 2 – To prepare for an evaluation of a mobile device to be used for the protection of Australian Government information at the PROTECTED Level – mobile device vendors should consult with ASD at the earliest opportunity. The product must successfully complete an evaluation at the UNCLASSIFIED/DLM level, and the product must also successfully complete an evaluation against the ASD Mandatory Requirements Addendum to the MDFPP.

Phase 3 - For a mobile device to be found suitable against the ISM's requirements for ICT equipment containing PROTECTED information to be handled at an UNCLASSIFIED level – Phase 2 must have been

successfully completed before vendors may request an ASD Cryptographic Evaluation (ACE) be carried out against the mobile device.

4. The ACE Process includes evaluation activities such as the following:

- Documentation Review: verifying the strength of the architectural design
- Source Code Review: verifying the correct operation of high risk functions
- Functional Testing: black-box or user testing of the product.

Certification

5. Only after successfully completing the three phases described above will ASD consider certifying a device as suitable for the protection of Australian Government information at the PROTECTED level.

6. The Evaluation Pathway for Mobile Devices and any supporting documents are subject to change. Potential vendors are advised to keep abreast of such changes by engaging with ASD.

7. ASD will recognise any evaluation, from a recognised Common Criteria scheme, completed against the MDFPP v 1.0 at the time of publication of this broadcast. Subsequently, ASD will then only recognise new evaluations against the most recently endorsed version of the MDFPP.

Further Information

8. The following references can be found on the ASD public website http://www.asd.gov.au:

- *The Australian Government Information Security Manual* (ISM)
- *Mobile Device Fundamentals Protection Profile,* version 1.1, dated 12 Feb 2014
- *ASD Mandatory Requirements Addendum,* version 1.0, dated 11 Mar 2014.

Contact Details

Australian Government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.

R17847024