INSTRUCTIONS ON THE ALLOCATION AND USE OF BLACKBERRY IN THE AUSTRALIAN GOVERNMENT

1. Introduction
Section 44 of the Financial Management and Accountability (FMA) Act 1997 requires the Chief Executive of each department and agency to promote the efficient, effective and ethical use of resources for which they are responsible. The Chief Executive is also responsible for the day-to-day management of their agency’s protective security arrangements (Protective Security Manual Part A, Section 1.3).

This instruction provides Chief Executives with guidance on the use of BlackBerry® personal electronic devices (PEDs) and on their interaction with agency electronic mail (email) systems. Should agencies decide to use any other PED, the policy requirements defined in the Australian Government Information and Communications Technology Security Manual (ACSI 33 paragraph 3.4.51) apply.

The demand for BlackBerry® has brought to a head the need for a consistent whole-of-government implementation of an effective email classification and protective markings system in Australian Government agencies. Protective markings help to regulate transmission of emails to hand-held and portable devices.

These instructions have been prepared with the assistance of the Defence Signals Directorate (DSD).

2. General
Under Defence Signals Directorate (DSD) ICT Security Policy for the Use of BlackBerry by the Australian Government:

a) BlackBerry may be used for the transmission and storage of X-In-Confidence and Restricted information. If an agency can demonstrate a business need for BlackBerry, the AGIMO guidance, supported by DSD, requires that agencies must:
   i. comply with the Defence Signals Directorate (DSD) ICT Security Policy on BlackBerry
   ii. implement the relevant requirements for email protective markings from the most current release of ACSI 33
   iii. implement the protective markings in accordance with the implementation guide and standards for email protective markings.

   Better Practice Guidance No. 23 – Use of BlackBerry® Devices, provides further detail.

b) BlackBerry must not be used for the transmission or storage of Cabinet-in-Confidence, Protected, Highly Protected, Confidential, Secret or Top Secret information.
c) BlackBerry may be used with ICT systems that process Unclassified, X-In-Confidence and Restricted information. If an agency can demonstrate a business need for BlackBerry, the AGIMO guidance, supported by DSD, requires that agencies must:
   i. comply with the Defence Signals Directorate (DSD) ICT Security Policy on BlackBerry
   ii. implement the relevant requirements for email protective markings from the most current release of ACSI 33
   iii. implement the protective markings in accordance with the implementation guide and standards for email protective markings.

Better Practice Guidance No. 23 – *Use of BlackBerry® Devices*, provides further detail.

d) BlackBerry should not be used with ICT systems that process Cabinet-In-Confidence, Protected or Highly Protected information. Agencies with a demonstrated business need for BlackBerry must meet the ACSI 33 requirements for deviating from a “should not” (paragraph 1.0.18). The AGIMO guidance, supported by DSD, requires that agencies must:
   i. comply with the Defence Signals Directorate (DSD) ICT Security Policy on BlackBerry
   ii. implement the relevant requirements for email protective markings from the most current release of ACSI 33
   iii. implement the protective markings in accordance with the implementation guide and standards for email protective markings
   iv. have the agency’s gateways configured to ensure that emails and attachments classified at Cabinet-In-Confidence, Protected or Highly Protected are not sent to/from BlackBerry.

In addition, the Chief Executive must:
   v. meet ACSI 33 requirements and have no waivers in place that are relevant to the proposed implementation of BlackBerry
   vi. have no outstanding issues from system security or security audit reports that are relevant to the proposed implementation of BlackBerry
   vii. have ICT systems certified and accredited in accordance with requirements of ACSI 33
   viii. undertake and complete a post implementation review of BlackBerry within 12 months.

Better Practice Guidance No. 23 – *Use of BlackBerry® Devices*, provides further detail.

e) BlackBerry must not be used with ICT systems that process Confidential, Secret or Top Secret Information.

3. Procedures and Guidelines
DSD policy on this topic is contained in the DSD *ICT Security Policy for the Use of BlackBerry by the Australian Government*, which is included at Attachment A.

The Better Practice Guidance No. 23 - *Use of BlackBerry® Devices* (Attachment B) provides detailed supporting procedures for the management and use of BlackBerry®.
Officers involved in the implementation or use of BlackBerry® devices shall also pay due regard to:

- Better Practice Guidance No. 24 – *User Requirements for BlackBerry® Devices (Attachment C)*;
- *Implementation Guide for Email Protective Markings for Australian Government Agencies*; and
- *Email Protective Marking Standard for the Australian Government*. 