DEFENCE SUBMISSION TO THE JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT (JCPAA) INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

Introduction

1. Defence is a significant creator and user of electronic information. The ability to effectively manage such information is a capability critical to the success of the Australian Defence Force in successfully completing its task of defending Australia's national interests. Consequently, the Federal Government has invested heavily in Defence's information management.

2. At the centre of this investment is the Office of the Chief Information Officer (OCIO). The CIO is a member of Defence's highest level committee, the Defence Committee, and reports directly to the Secretary and the Chief of the Defence Force (CDF). The role of the CIO has just been enhanced to provide the resources for the CIO to act as the coordinating capability manager for the Defence Information Environment, the single entity that encompasses all of Defence's information capabilities. Among the CIO's assigned tasks is the establishment of an effective governance regime for the Defence Information Environment. This task includes the management and integrity of electronic information.

Defence's Electronic Information Management

3. Defence's electronic information may be broadly described as taking one of two forms: information relating to national security and more generic information relating to Defence's role as a large public service department. Information relating to national security is held on information systems that are not accessible to those without a positive need to know. Access to these systems is tightly controlled and regulations are rigorously enforced. Further description of this information or its management would require a security classified submission and as the inquiry's terms of reference refer specifically to the more generic information, it is on that information that this response will concentrate.

4. There are three Defence-wide enterprise business processes which collect, process and store information. They cover the fields of material and logistic support, financial management and human resource management. Each of these processes has an identified owner at the SES Band 2 or higher level (or the military equivalent). For each process there is also an appointed domain chief information officer. The responsibilities of the enterprise business process owner (EBPO) specifically include accountability for the privacy, confidentiality and integrity of information. These arrangements are detailed in joint agreements between the CIO and each of the EBPOs.

5. The governance of these arrangements is supported by a series of policies that define the standards for information management. These policies are readily accessible, widely publicised and are the subject of a suitable maintenance regime. Governance of the Defence Information Environment is also regularly considered by the Defence Information Environment Committee, which meets monthly and is chaired by the CIO. This committee provides advice to the CIO to assist him to meet his responsibilities to the Secretary and the CDF, for information management.

6. The standards for information management security are defined in Defence's security manuals. These are based on the Commonwealth's *Protective Security Manual*. The enterprise information systems that support the enterprise business processes are being accredited to these standards. The human resource management information system, which contains the majority of the data of interest to the Inquiry, has recently received accreditation.

7. Across Defence, information management is supported by Defence's information systems infrastructure. This infrastructure is characterised by:

a. accredited architecture adhering to a system of regulatory controls;

b. robust border protection of the Defence networks;

c. robust internal protection against degradation;

d. encryption of internal transmission channels;

e. rigorous and layered access control based on a need to know;

f. routine monitoring of user activity; and

g. routine audit.

Legislative Framework

8. Defence believes that the current legislative framework is adequate. However, in the broad area of archiving, Defence notes that the technology that supports current electronic information has a lifetime considerably shorter than the period for which archives need to be maintained. Support of such technologies is unlikely to be possible over the archive maintenance period. Backward compatibility is not always a feature of new technologies and where it does exist it can be expensive. The effect of these complications should be considered when such legislation is reviewed.

Summary

9. Defence manages the electronic information that it collects, processes and stores on behalf of the Commonwealth in a manner that ensures its privacy, confidentiality, integrity and security.