Australian Government

Department of Finance and Administration

Dr Ian Watt
Secretary

Our Ref: ISEC002336

Mr James Catchpole
Committee Secretary
Joint Statutory Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Mr Catchpole

Government Response to the Joint Committee of Public Accounts and Audit Report 399: Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

Further to the advice provided to you on 9 September 2004 by Ms Robyn Fleming, General Manager, Policy and Strategy Branch, Australian Government Information Management Office, please find attached the administrative response to the above report.

I would appreciate you submitting the attached response to the new Chair at the appropriate time.

If you have any enquiries regarding the administrative response please contact Ms Fleming on Tel: 6271 1513.

Yours sincerely

I J Watt
14 January 2005

EXECUTIVE MINUTE

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT
REPORT No. 399
Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

General Comments

The Department of Finance and Administration notes the Joint Committee of Public Accounts and Audit (JCPAA) Report 399 on the *Inquiry into the Management and Integrity of Electronic Information in the Commonwealth* (the Report). The Government is reliant on information and communications technology (ICT) to store and share information as well as to inform and transact with individuals, businesses and groups. Secure storage of information and the privacy, confidentiality and integrity of data are responsibilities of all Government departments and agencies.
Under the Government's operational framework, responsibilities are allocated to the Chief Executive of each department and agency. At the core of each department and agency's accountability is an obligation to comply with the *Financial Management and Accountability Act 1997* (the FMA Act).

In addition to these statutory financial accountability measures, all departments and agencies must meet minimum protective security standards as set out in the Protective Security Manual (PSM). The PSM requires that all Government departments and agencies should apply the standards set out in the Australian Communications-Electronic Security Instruction 33 (ACSI 33) for the protection of information stored and transmitted using their information and communications systems.

In the dynamic ICT environment, the Government's information security and management frameworks are regularly reviewed and refreshed to support departments and agencies to meet the challenges associated with ICT management and security. The PSM and the Government's Public Key Infrastructure (PKI) strategy, *Gatekeeper*, are to be reviewed within the next six months. ACSI 33 is reviewed quarterly. The recommendations of the JCPAA will be taken into account in these review processes.

Many of the existing policy frameworks for ICT management and security intersect, and responsibilities can span several portfolios. The Government established the Information Management Strategy Committee (IMSC) in 2002 to provide leadership on whole of government ICT issues. The IMSC provides a focal point for many of the matters raised in the Report.

This document provides a whole of government response to the recommendations of the Report. Departments with lead-agency responsibility for each of the recommendations of the JCPAA are listed below. Responses to the individual recommendations are attached.

Agency Roles

The lead-agency role for each response to the recommendations is shown below. This reflects current Administrative Arrangement Orders (AAOs). In particular, the Australian Government Information Management Office (AGIMO) has become a business group in the Department of Finance and Administration (Finance). Consequently Finance now has the lead agency role in relation to several of the recommendations of the JCPAA.

Recommendation 1 - The Attorney-General's Department is the lead agency. The Defence Signals Directorate (DSD) has assisted the Attorney-General's Department.

Recommendation 2 –Finance is the lead agency. The Attorney-General's Department has assisted Finance.

Recommendation 3 – The Department of the Prime Minister and Cabinet is the lead agency.

Recommendation 4 - Finance is the lead agency.

Recommendation 5 - The Attorney-General's Department is the lead agency (rather than AGIMO as indicated in the Report). DSD and Finance have assisted the Attorney-General's Department.

Recommendation 6 - The Attorney-General's Department is the lead agency (rather than AGIMO as indicated in the Report).

Recommendation 7 –Finance is the lead agency. The National Archives of Australia (NAA) has assisted Finance.

Recommendation 8 - Finance is the lead agency, with advice from the Australian National Audit Office (ANAO) and assistance from the Attorney-General's Department.

Recommendation 9 –Finance is the lead agency (rather than the Department of the Prime Minister and Cabinet as indicated in the Report).

Responses to the Recommendations

Recommendation 1
The Defence Signals Directorate (DSD) in conjunction with other agencies where appropriate, ensure that Commonwealth agencies institute without delay, physical security plans for each of their information technology systems. Additional plans may be necessary for key information technology centres. DSD to advise the Committee within six months of the tabling of this report, on the status and adequacy of these plans.

Supported in principle.

The Protective Security Manual (PSM) requires the Chief Executive of each department and agency to implement physical security plans for all their sites, including those that contain information and communications technology (ICT) systems, and to report annually to Government on these plans. The Government requires all departments and agencies to comply with the PSM. It is the responsibility of each Chief Executive to ensure that this occurs.

The Protective Security Coordination Centre (PSCC) in the Attorney-General's Department is responsible for setting whole of government security policy and monitoring compliance. PSCC is the appropriate organisation to implement the Recommendation, rather than the Defence Signals Directorate (DSD). Departments and agencies may draw on the DSD for advice regarding ICT security issues. The Australian Security Intelligence Organisation may also be called upon to assess the adequacy of physical security measures.

The PSM is being revised and the PSCC will ensure that the requirement for physical security plans for ICT systems is reinforced in the new edition.

The PSCC monitors agency compliance with Government policy through an annual self-assessment survey by all departments and agencies. The next survey is due in February 2005 and the PSCC will ensure that the survey requires advice from departments and agencies on their compliance with physical security requirements for ICT systems. The PSCC reports on the outcomes of these surveys to the National Security Committee of Cabinet. Due to the scheduling of the survey, it will not be possible to report in the timeframe requested by the Joint Committee of Public Accounts and Audit (JCPAA). A report will be provided to the JCPAA within two months of the completion of the survey.

Recommendation 2
The Australian Government Information Management Office, advise all Commonwealth agencies that new or renegotiated contracts for outsourcing of information technology services need to pursue best practice and include the following:

- clear information sharing protocols that require each party to inform the other when an information technology security incident occurs that, directly or indirectly, affects the security of agency information technology networks;
- prohibition of unauthorised subcontracting of information technology services;
- provision for a graduated hierarchy of sanctions in response to security breaches.

Supported.

In May 2004, the Australian Government Information Management Office (AGIMO) released *A Guide to ICT Sourcing – Developing and Executing an ICT Sourcing Strategy.* This publication encourages best practice by departments and agencies in the procurement of ICT. The next edition of the *Guide* will reflect the requirement that sourcing strategies comply with PSM obligations and the best practice contractual issues raised by the Committee.

The PSM provides guidance to departments and agencies on their entitlement to terminate an ICT contract if there is a failure to comply with security requirements specified in the contract. It also advises agencies to consider alternative options in relation to sanctions, such as the use of a graduated response depending on the type of information that the security incident relates to, the number of incidents within a designated period and the likely consequences of continued incidents.

The PSCC will reinforce security requirements around ICT sourcing in the next edition of the PSM, and also intends to publish a better practice guide on security issues in relation to contracting, including ICT contracting.

Recommendation 3
The Department of Prime Minister and Cabinet introduce regulations that address the issuing and use of laptop computers and other portable electronic devices by Commonwealth agencies. The regulations should require that:

- such equipment is only issued to officers on a needs basis;
- such equipment is assigned to an individual, rather than to a work area, to ensure clear accountability;
- portable electronic devices are given password protection and, where they hold sensitive information, that data should be suitably encrypted;
- movement logs are made mandatory for valuable equipment taken outside agency premises ('valuable' here includes the significance of the information involved, as well as the monetary value);
- all thefts are reported to the police and to a central reporting body such as the Defence Signals Directorate; and
- regular inventory audits are conducted.

Not supported.

It is the responsibility of the Chief Executive of each department and agency under sections 44 and 52 of the *Financial Management and Accountability Act 1997 (*FMA Act) to promote the proper use of Commonwealth resources for which they are responsible, and to ensure that they have appropriate controls in place.

The Government is of the view that these arrangements are sufficient and does not consider it necessary to further regulate the controls required for the issuing and use of laptop computers and other portable electronic devices. Chief Executives are best placed to determine which risk-based controls are most appropriate to their specific operations for the protection of portable electronic devices and the information stored on them. Chief Executive Instructions issued in each department and agency require that:

- portable equipment be issued to officers on a needs basis;
- equipment be assigned to an individual, rather than to a work area, to ensure clear accountability; and,
- regular inventory audits be conducted.

In addition, controls prescribed by Australian Communications-Electronic Security Instruction 33 (ACSI 33) and the PSM require departments and agencies to:

- configure portable electronic devices with encryption software and a lock that requires the user to authenticate before the agency's ICT system can be used;
- implement controls for the movement and transport of equipment containing security classified information; and,
- ensure that Agency Security Advisers and ICT Security Advisers report significant computer incidents to the DSD.

In terms of reporting, the Government has established:

- the Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) through which departments and agencies report the loss of ICT equipment, and which supports the reporting of thefts of ICT equipment to the Australian Federal Police; and,
- OnSecure, a restricted website that allows departments and agencies to securely report information security incidents online. This scheme allows the DSD to analyse incident reports and identify developing patterns arising from these incidents.

Recommendation 4
The Australian Government Information Management Office (AGIMO) ensure that Commonwealth agencies:
- have up-to-date asset registers of all IT equipment owned by them and used on their premises; and
- undertake a regular audit and reconciliation program of all owned and leased IT equipment.

AGIMO should advise the Committee, in an Executive Minute, of the completeness of the registers and the audit procedures that have been established.

Not supported.

It is the responsibility of the Chief Executive of each department and agency under sections 44, 48 and 52 of the FMA Act to promote the proper use of Government resources for which they are responsible, and to ensure that they have asset registers and audit programs in place. In terms of leased ICT equipment, each department and agency should have clauses within their contracts that ensure completion of asset registers and audit programs.

Each department and agency audit committee should review the adequacy of these processes. The Government is of the view that these arrangements are sufficient.
The Department of Finance and Administration (Finance) will publish examples of best practice for departments and agencies in maintaining their asset registers of ICT equipment and undertaking regular audit and reconciliation programs of ICT equipment.

Recommendation 5
The Australian Government Information Management Office, in consultation with the Defence Signals Directorate, reiterate to all Commonwealth agencies their responsibility to comply with the reporting requirements of the Information Security Incident Detection, Reporting and Analysis Scheme particularly the mandatory reporting of category 3 and category 4 incidents.

Supported.

The PSCC is responsible for setting whole of government security policy and monitoring compliance and has primary carriage of these issues.

Finance will develop a better practice checklist for agency reporting requirements under the ISIDRAS reporting scheme in consultation with the PSCC and DSD. This checklist will be circulated to all departments and agencies.

The PSM is being revised and the PSCC will ensure that the reporting requirement for ISIDRAS is reinforced.

The Government has also established OnSecure, a restricted website that allows Government departments and agencies to securely report information security incidents online rather than by mail or facsimile. The site allows DSD to analyse incident reports more quickly and effectively to identify any developing patterns and to assess the resulting threat level.

Recommendation 6
The Australian Government Information Management Office (AGIMO) monitor and report on the performance of Commonwealth agencies:
- implementation and maintenance of a flexible and responsive security risk management strategy for IT networks including hardware, software and data protection; and
- maintain an awareness of current and emerging threats to their computer networks and the recommended countermeasures.

AGIMO should advise the Committee in an Executive Minute, of the status and completeness of these arrangements.

Supported in principle.

A responsive security risk management strategy for information technology networks has been implemented and managed through the PSM that requires the Chief Executive of each department and agency to implement security risk management strategies, develop security plans for all aspects of their ICT networks and report annually to Government on their compliance with these requirements. All departments and agencies are required to comply with the PSM. It is the responsibility of each Chief Executive to ensure that this occurs.

The PSCC is responsible for setting whole of government security policy and monitoring compliance, and is the appropriate organisation to implement the recommendation, rather than Finance.

The PSM is being revised, and the PSCC will ensure that the requirement for security risk management strategies and security plans for all aspects of their operations, including ICT systems, is reinforced.

Awareness of threats and treatment measures is a fundamental part of risk management. The PSM mandates the application of the Australian and New Zealand Standard 4360:1999 *Risk Management* process to protective security risk management, which incorporates information systems security issues. In addition, the OnSecure website provides a single Government internet site for online security material.

Regarding alerts, departments and agencies may also subscribe to AusCERT - the national Computer Emergency Response Team for Australia - which is an independent not-for-profit organisation based at the University of Queensland. AusCERT operates an Early Warning Alert Service to help members identify and respond to the most critical security threats and vulnerabilities by identifying those which require urgent consideration and action. It also operates an incident reporting scheme. The Government considers this is sufficient and there is no basis for duplicating this process.

Recommendation 7
The Australian Government Information Management Office (AGIMO), with support from the National Archives of Australia (NAA), ensure that Commonwealth agencies implement knowledge management and archival policies such as e-permanence which give equal priority to preserving electronic and paper-based records. AGIMO to advise the Committee, in an Executive Minute, of the status of these arrangements. The NAA to be resourced properly.

Supported in principle.

The National Archives of Australia (NAA) has responsibility for archival policy, and its e-permanence policies are actively promoted across Government departments and agencies. Over the past four years the NAA has issued an extensive suite of guidelines for dealing with web-based and other digital records. In May of this year, it issued for comment draft *Guidelines for Creating, Managing and Preserving Digital Records*, as well as a *Self-Assessment Checklist*. The NAA is considering possible changes to update the administrative measures within the *Archives Act 1983* in accordance with current best practice and to strengthen the role of the NAA in promoting good record keeping across Government departments and agencies.

The IMSC is also supporting the development and implementation of knowledge management practices for application across the Australian Public Sector. Finance is working towards a better understanding and application of knowledge management through projects sponsored by the IMSC such as a new Communities of Practice initiative and, in conjunction with the NAA, a better practice checklist for digital recordkeeping.

The Government is of the view that these arrangements are sufficient to address the JCPAA's recommendation.

Recommendation 8

The Australian Government Information Management Office (AGIMO), in consultation with the Australian National Audit Office, ensure that Commonwealth agencies have in place comprehensive and tested business continuity and disaster recovery plans for their electronic records networks and services. AGIMO to advise the Committee, in an Executive Minute, of progress with the implementation and testing of these plans.

Supported in principle.

Chief Executives of departments and agencies are responsible for the secure operation of their functions, including continuity or recovery of services potentially affected by a disruption or disaster. The IMSC is sponsoring development and promulgation of best practice in business continuity and business recovery planning to assist departments and agencies share experiences and solutions.

The recent Australian National Audit Office Audit (ANAO) report, *Control Structures as part of the Audit of Financial Statements of Major Australian Government Entities for the Year Ending 30 June 2004*, found a significant improvement in business continuity management in major Government entities over the previous year. The ANAO reported that this reflects the significant progress most entities have made towards the development of effective business continuity and business recovery plans in recognition of the increased risk of potential disruption to service delivery. The Government is of the view that existing arrangements are sufficient to address the Committee's recommendation.

The PSM recommends that security risk treatments should, where appropriate, include continuity plans as mechanisms for reducing the adverse consequences of a security risk. The PSM also refers departments and agencies to the Emergency Management Australia publication *Non-stop Service: Continuity Management Guidelines for Public Sector Agencies* and, in relation to physical security issues, Australian Standard 3745-1995: *Emergency Control Organisation and Procedures for Buildings.*

The PSM is being revised and the PSCC will ensure that the need for comprehensive and tested business continuity and disaster recovery plans for electronic records networks and services is reinforced in the new edition.

The ANAO also has produced the Better Practice Guide, *Business Continuity Management "Keeping the Wheels in Motion"*, to assist departments and agencies understand business continuity management concepts in a risk management context. The guide identifies the processes and procedures required to be undertaken to produce a business continuity plan, recognising that a robust continuity plan comprises many elements including, but not limited to, business continuity and business recovery plans for ICT which support service delivery.

Following the 2003 Canberra bushfires, AGIMO, under the auspices of the IMSC, convened forums in which departments and agencies shared their experiences in relation to the impact of the fires on their ICT arrangements. This process identified a number of areas in which assumptions underpinning the ICT components of business continuity and business recovery plans warranted review. These included matters such as the robustness of backup power supplies, the availability of technical support staff and the minimum geographical distance between ICT systems and remote backup facilities.

These "lessons learned" were shared among departments and agencies to inform their business continuity and business recovery planning processes. Finance will further support departments and agencies by developing a best practice checklist based on these lessons.

Recommendation 9
The Department of the Prime Minister and Cabinet should review and report to the Committee on the cost effectiveness of Gatekeeper versus other commercially available public key infrastructure products and systems.

Supported in principle.

Finance will coordinate a review of the *Gatekeeper* strategy and report its findings to the Committee.

Gatekeeper is the Government's strategy for the use of Public Key Infrastructure (PKI) by departments and agencies. *Gatekeeper* provides the policies and standards for the provision of digital certificates which include "Evidence of Identity" protocols, certificate issuing, security, business processes and risk management. Commercial providers of certificates are accredited against these policies and standards. The standards nature of *Gatekeeper* precludes measurement of its cost effectiveness in comparison to commercially available products and technologies.

There are commercially available authentication products and systems that support PKI or other authentication approaches such as username and password. The business case for Government use of these products is examined in the *Australian Government e-Authentication Framework*, which is currently under development. An exposure draft seeking comment on the *Framework* was publicly released in May 2004. Under the *Framework*, departments and agencies are encouraged to implement authentication mechanisms appropriate to the level of risk in a transaction. PKI would be used only when warranted by risk. Nevertheless, when using PKI to authenticate external clients, Australian Government departments and agencies are required to use those solutions that are *Gatekeeper* compliant.

The review of *Gatekeeper* will be undertaken in association with relevant stakeholders. The review is scheduled to be completed by the end of the 2004-05 financial year.

I J Watt

14 January 2005