18 December 2002

Dr John Carter
Inquiry Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

www.aph.gov.au/house/committee/jpaa/index.htm

Dear Dr Carter,

I refer to Ms Kerley's letter of 28 October 2002 to Dr Calvert concerning the inquiry into the management and integrity of electronic information in the Commonwealth by the Joint Committee of Public Accounts and Audit. Dr Calvert has asked me to reply on his behalf.

I welcome the invitation for the Department of Foreign Affairs and Trade to provide a written submission to the Committee on the Management and Integrity of Electronic Information in the Commonwealth. The attached submission highlights the department's responsibility for managing sensitive data such as consular cases and passport information, as well as providing secure infrastructure for the "whole of government" international telecommunications network. We take pride in providing a high level of electronic data management and security.

If your secretariat has any queries about the information contained in the department's submission, we would be pleased to respond to them. The contact officer in the department is Mr Frank Evatt (phone 62611539 email: frank.evatt@dfat.gov.au).

I wish to take this opportunity to wish the Committee well with its inquiry.

Yours sincerely

Paul Tighe
First Assistant Secretary
Diplomatic Security, Information Management
and Services Division

THE DEPARTMENT OF FOREIGN AFFAIRS AND TRADE

Submission to the Joint Committee of Public Accounts and Audit

Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

Version 1.0 18 December 2002

Department of Foreign Affairs and Trade
Information Management Branch
RG Casey Building
John McEwen Crescent
BARTON **ACT** 0221

Content

Page

Inquiry into Management and Integrity of Electronic Information in the Commonwealth

The Department of Foreign Affairs and Trade (DFAT) appreciates the opportunity to make a submission to the Joint Committee of Public Accounts and Audit highlighting the measures taken to maintain a high level of protection of electronic information in the department.

The department's IT infrastructure is designed to provide a "whole of government" secure international communications network. Therefore much of the information transmitted on the network originated in, and is being used by, other government agencies. This submission addresses the management and security arrangements for information systems that originated in DFAT.

The aim of DFAT is to advance the interests of Australia and Australians internationally. It is, therefore, imperative that the department maintains a robust security culture in order to achieve this objective. To do this effectively employees need to work in an environment of trust, integrity and a high degree of security awareness and vigilance in protecting official information.

All DFAT employees and cleared contract staff are required to sign annually a written declaration that they have read a statement of security responsibilities and that they understand that the unauthorised disclosure of official information is an offence under the Crimes Act, punishable by up to two years imprisonment. Documentation concerning appointments in DFAT establish a clear-cut rule that employment is dependent on an employee having a valid security clearance.

The integrity of the department's electronic information security and management protocol is fundamental in the delivery of foreign policy advice to the Government and consular and passport services to the Australian community. This is of particular importance because of the national security implications or very private and personal nature of much of this information. The department takes seriously its responsibility to protect and safeguard electronic data on private citizens.

IT Governance Arrangements

Effective governance arrangements are important to provide senior management with clear visibility of programs and projects, and help them ensure that common goals, objectives and technical standards are applied across the department as a whole and across the system it manages. They also allow more effective long term planning, encourage application of best practice management, and assist compliance with national security and IT security requirements.

DFAT conducted a review of the department's management of information technology in September 2000. The review noted the need to strengthen its internal governance arrangements. New IT governance arrangements were designed and implemented to ensure a coherent and cost-effective approach to IT management and decision making across the department as a whole.

The governance arrangements focus on the Information Technology Strategy Committee (ITSC). The ITSC is chaired by the First Assistant Secretary, Diplomatic Security, Information Management and Services Division who is also designated Chief Information Officer. The ITSC reports to the department's Senior Executive and supported by a Technical Advisory Group and the Consultative Committee on Information Management, which represents IT users in the department.

IT Development

DFAT is in the middle of a major deployment of its Secure Australian Telecommunications and Information Network (SATIN) to Australian diplomatic and consular missions. SATIN is replacing ADCNET (the Australian Diplomatic Secure Network) which for the past decade has been the government's secure international communications network.

Deployment of SATIN also requires an upgrade of bandwidth links to overseas missions to support the enhanced software the additional infrastructure requires. Included in the upgrades are the advanced security measures to protect the integrity of the network data. The SATIN deployment program is scheduled to be completed in the 2004/05 financial year.

Enhancing the department's wider IT applications to meet business needs is proceeding as resources permit. Some business applications are still in the development or pilot stage and are expected to come on-line next year or when the SATIN deployment is completed.

Business Applications

The main business applications that contain information on Australians are the:

- Passports Issues and Control System (PICS)
- Consular Management Information System (CMIS)
- International Cablegram System
- Financial Management Information System (SAP)
- Human Resource Information System (PeopleSoft)
- Graduate Recruitment System

The privacy, confidentiality and integrity of the Commonwealth's electronic data

DFAT takes its custodianship of Commonwealth data seriously. It has a clear focus on the privacy, confidentiality and integrity of this electronic data. DFAT fully understands and complies with its obligations under the Privacy Act (1988) and, in accordance with the Protective Security Manual (PSM) and the Defence Signals Directorates (DSD) publication, ACSI 33, has implemented a threat and risk analysis approach to providing IT protective security measures. The department's internal policy documentation such as Administrative Circulars, DFAT Security Instructions and the various Acceptable Usage Policies (e.g. Email Acceptable Usage Policy) codify the department's adherence to the legislative framework.

General Protective Measures:

DFAT provides the following types of protective measures for electronic data:

- procedural training and security awareness for staff
- access controls on IT systems limiting access to suitably authorised users only
- policy and procedural documentation for IT support, maintenance and backup strategies
- policy and procedural documentation for business continuity strategies
- implementation of auditing procedures and data integrity checks
- configuration control procedures for all IT systems
- system redundancy (eg duplication of mission critical resources and alternative communications paths)
- an administrative requirement to purchase approved hardware and software from recognised vendors (eg Evaluated Products List provided by DSD)
- provision of a Standard Operating Environment (SOE) across the department using tested and reliable software
- implementation of a proactive antivirus strategy
- the certification of systems as 'fit for purpose' by external agencies such as DSD

Segregation of Information

The primary form of protection is the segregation of information into information that deals with national security or highly classified matters, and information that is unclassified or classified at a low level. Both systems are being replaced by SATIN. SATIN Low replaces the NNS (Non-National Security) system and SATIN High replaces the secure ADCNET system. The SATIN network is logically and physically segmented and allows the user to operate both systems from a single desktop unit. Access to each system is controlled by personal user identification passwords.

Access to applications within SATIN is controlled on a "need-to-know" basis by suitably trained and security cleared staff.

Major IT and Data usage and storage systems in the Department:

DFAT maintains a significant number of separate IT/IM systems and applications. Following is a summary of these systems and the methods used to protect this data.

Passport Issue and Control System (PICS)

- Operates on Non-National Security and SATIN Low.
- The system contains personal data on Australian passport applicants including: Name, Address, DOB, Gender, Identity Validation, NOK etc.
- Size of Holding: 225 Gb.
- Data storage is outsourced.
- The data is stored on a mainframe computer.
- A vendor security vetting process and a physical security site survey have been conducted.
- All staff with access to the data are security cleared and system access is controlled by IBM Discretionary Access Control System.

Consular Management Information System (CMIS)

- Operates on Non-National Security and SATIN Low.
- The system contains information on current consular cases. It also includes the Online Register of Australians and a Temporary Emergency Consular System.
- The CMIS system runs on servers which are located in a physically secure, purpose built computing room with audited access control. Logical access control to the data is on a "need-to-know" basis, administered by Systems Administrators on behalf of the CMIS manager, Director Consular Operations Section, Consular Branch. Only authorised users who are suitably cleared have access to CMIS. Views of the data are restricted on an individual basis and are fully audited. CMIS is backed up using the department's off-site on-line system to a secure location within Canberra.

Cable System

- Two systems- National Security and Non-National Security and SATIN High and Low.
- The formal messaging system carries traffic to and from DFAT, overseas missions, state offices and Commonwealth agencies.
- The cable network in a closed network where all messages are registered and the distribution strictly controlled.
- The cables are distributed on a "need-to-know" basis including to other departments and ministers' offices.
- Size of Holding: Satin High - 850 Mb, Satin Low: 218 Mb.

Financial Management Information System (SAP)

- Non-National Security and SATIN Low.
- Size of Holding: 2.5 Gb.
- Vender information in relation to financial data of the department including principal accounting records, journals and ledgers. SAP also facilitates the collection and provision of financial information to Federal and State Government agencies operating overseas.
- Strong user authentication, which requires a password account on the SAP system as well as a standard DFAT user account. The SAP data are stored in a physically secure, purpose built computing room with audited access control. The data are backed up to the department's SAN storage facility on a nightly basis.

Human Resources Information System (PeopleSoft)

- Non-National Security and SATIN Low.
- Size of Holding: 9 Gb.
- Staff's Personnel information including next of kin records.
- Strong user authentication, which requires a password account on the PeopleSoft system as well as a standard DFAT user account. The PeopleSoft data are stored in a physically secure, purpose built computing room with audited access control. The data are backed up to the departments SAN storage facility on a nightly basis.

Graduate Recruitment System

- Non-National Security and SATIN Low.
- On-line web based system to manage graduate recruitment.
- Data include biographical and educational data on graduate applicants.
- Size of holding 234 Mb.
- A web based application encrypted of in-transit data. The data are stored securely in a database protected by a firewall. When registering, applicants, establish a logon identity with a username and password.
- User access is restricted on a "need-to-know" basis.
- The data are backed up to the department's SAN storage facility on a nightly basis.
- For audit purposes the data are held for a minimum of 3 years.

The management and security of electronic information transmitted by Commonwealth agencies

The Department of Foreign Affairs and Trade, as the owner of the Government's global secure communications network, provides the communications backbone for the Government's international operations. The network provides secure communications links to 11 government agencies and seven ministers' offices in Australia and 86 locations overseas (Annual Report 2001-2002 p 101).

The department provides the following protective measures for electronic transmission of data;

- Encryption of external data links, using Government furnished equipment.
- Ensuring a high standard of physical security for all installations of the department's network equipment.
- Logical and Physical access control on all network equipment both within Australia and overseas.
- Extensive security awareness training for all staff having access to the equipment.
- Full audit of all access to network equipment through a Network Management System.
- Involving DSD in the development of security critical components of the network such as the Secure Cable Gateway (SCG).
- Implementation of proactive antivirus and intruder detection strategies on any public interface to the department's network.

The management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks

The department's Five Year Information Technology Plan sets a number of management objectives concerning the security and storage of data. It seeks to ensure appropriate security of IT infrastructure, in both the IT and national security senses, with regard to the confidentiality, integrity and availability of information.

The department has been successful in managing the new security environment with its new challenges, such as the growing interconnectivity and communications with entities outside the department's network.

To maximise the capacity for effective network management and planning a new network management system was introduced which greatly increases its monitoring and fault finding capability.

A recent independent IT infrastructure audit concluded that DFAT's Storage Area Networks (SAN) configuration accords to best practice. The current configuration was mandated by the requirement that the SANs withstand the loss of the computer rooms without losing access to the data.

In the event of core switch or disk array failure, the SAN can be run in "failover" mode, which uses the secondary infrastructure and without any loss of data accessibility and negligible performance overhead. The failover mechanism for the SANs is a manual procedure. While this is not optimal from an operational point of view, this is an industry-wide limitation imposed by current SAN technologies.

The adequacy of the current legislative and guidance framework

The legislative and guidance framework contained in the Privacy Act (1988), the Protective Security Manual (PSM), the Australian Communications Security Instructions (ACSI) 33 and the Online Security initiatives of NOIE, is both comprehensive and challenging. Other important references include the *Crimes Act 1914* (sections 70 and 79) and the Australian Public Service Code of Conduct (section 13 of the *Public Service Act 1999*).

The department considers the range of existing guidelines and legislation pertaining to the management and integrity of electronic information, to be adequate. The mandatory compliance with the 'Information Privacy Principles' is considered adequate but not onerous and the 'Australian Communications Security Instructions (ACSI) 33' guidelines are used extensively when proposing departmental policy and procedures for IT security and data protection.

There have been two major reviews of the department's IT/IM systems in recent years. The 1998 Information Management Strategy paper linked the department's IT/IM management with the Corporate Plan. The business imperatives from the Corporate Plan define the vision for the department's Information Management services.

The September 2000 Information Technology Review recognised the importance of new forms of business and community interaction that have emerged as defining characteristics for the department's IT planning. This review identified specific risks facing the department. IT Security was seen as a key issue for DFAT and the review addressed approaches to deal with both the costs and complexities generated by the department's unique needs.

As a result of these reviews information technology governance arrangements were amended to included the appointment of the First Assistant Secretary, Diplomatic Security, Information Management and Services Division as the department's Chief Information Officer, and the creation of the Information Technology Strategy Committee which meets quarterly and reports to the Senior Executive on the strategic IT/IM needs of the department.