Optus Submission to the Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

January 2003

1. Overview

1.1 Optus welcomes the opportunity to provide this submission to the Joint Committee of Public Accounts and Audit's inquiry into 'The Management and Integrity of Electronic Information in the Commonwealth'.

1.2 Optus has a great deal of experience in providing products and services that process, store and transmit electronic information on behalf of the Commonwealth.

1.3 Our submission will provide details of the products and services Optus supplies to the Commonwealth as well as other governments and organisations. It will then detail a set of principles that Optus views as important in successfully managing the network security of electronic information on behalf of the Commonwealth.

1.4 Our submission also identifies deficiencies in the current security guidance framework and recommends the Committee consider the following recommendations:

- A more consistent approach to IT security standards and clearances between Commonwealth, State and Territory Governments and industry.
- The development of a more efficient, cost effective system to determine suitable products for the Defence Signal Directorate's (DSD) Endorsed Product List (EPL).
- The addition of a new level of security classification for the treatment of personal information currently classified under the 'non-national security' classification.
- Recognition in the Attorney Generals Department's Protective Security Manual (PSM) that the internet has a higher level of risk than a private carrier network.
- The value and level of classification of information should be considered in light of what an attacker must go through in order to compromise the information being carried on a network.
- Over classifying information and classifying all information at the highest level requires additional countermeasures and higher costs for both the Commonwealth and the carrier for questionable benefit.

2. Optus' Services and Products

Network Security

2.1 As part of our 'Managed Data Network Service' that is supplied as a component of Optus' Commonwealth Government Cluster 3 Outsourcing obligations, Optus supplies an 'Internet Protocol Security Service'.

2.2 All data that travels through this network is encrypted and satisfies security requirements to the classification of 'Protected'.

2.3 In order to provide this service the following elements are required:

- Provision and operation of a secure environment certified by DSD (Defence Signals Directorate) and ASIO;
- Access to people who have the skill, expertise and appropriate security clearance to be able to manage the network and the encryption keys; and
- Infrastructure to support Internet Protocol Security (IPSec) encryption employed on the network data transmissions.

OPI Trust

2.4 OPI Trust is a highly secure remote access service through the Optus Private Internet Protocol (OPI) Network to the customer's network.

2.5 OPI Trust uses public key infrastructure (PKI) and smart card technology with strong encryption to authenticate users and protect data.

2.6 The security enforcing components of OPI Trust provided by ActivCard are under evaluation to Common Criteria (CC) EAL2 and these are listed on the Defence Signals Directorate (DSD) Evaluated Products List (EPL). The digital certificates provided on the OPI Trust smart card can be supplied fully NOIE Gatekeeper compliant if required by a customer.

2.7 Customers can access the service via the internet, or via dial-up access through Optus points of presence throughout Australia.

2.8 OPI Trust is targeted at organisations that are working with very sensitive information. Examples include: federal, state and local governments, medical practitioners, lawyers, law enforcement agencies, and banking and finance institutions.

2.9 OPI Trust's current customers include two federal law enforcement agencies, a state/territory government and two of the four major Australian banks.

Managed Firewall Services

2.10 Managed firewall services provide protection to enterprise networks connected to the internet or other potentially hostile networks.

2.11 This service normally includes a Virtual Private Network (VPN) capability (see Managed IP-VPN below), so it is cost effective to provide both services using the same central equipment.

2.12 Associated services that can be optioned include intrusion detection systems, email screening and URL blocking.

2.13 Most firewalls offered under the service are either evaluated or under security evaluation for inclusion on the DSD EPL.

2.14 There are a number of security appliances available from different manufacturers intended to cover the full range of Optus customers:

- NetScreen – SOHO to SMEs. (Under security evaluation)
- Nokia/Checkpoint – intended for SME through to larger corporations. (Some versions are under security evaluation)
- CyberGuard – Large Corporations and Government Agencies (Evaluated to CC EAL4 and ITSEC E3)

Managed IP-VPN Services

2.15 The Optus Managed IP-VPN (Internet Protocol -Virtual Private Network) service enables an organisation to establish a secure data network across the internet without using expensive private or leased circuits.

2.16 Managed IP-VPN provides secure connections to branch offices, customers, trading partners and employees anywhere in the world.

2.17 This service is suited to customers that require connections between multiple sites or remote access for employees.

3. General Observations

3.1 Optus supports the following principles as important in the management of information on behalf of Commonwealth agencies:

- Network security should be managed as a complete system rather than a set of individual elements.
- Recognition of the many points and types of risk in the protection of electronic data through the process of collection, transmission and storage.
- Protection of data is only as effective as the measures in place to protect the weakest link. For example, a system can have the most stringent measures in place to secure the network, only to have that 'wasted' if the systems on which the data resides are easily accessed or hacked.
- Continuous encryption of data from collection, transmission to storage. For example, a network will not be secure if the carriage service is encrypted but the network device on which this service is terminated is not encrypted.
- An effective compliant management regime for network systems. This regime should be supported by systems that have privilege levels for defining and managing the degree of control and access available to individuals as well as logs to track and record all activities.
- Consistency of security standards applied to the transmission of Commonwealth derived personal information to both service providers and state and territory agencies.

- An appropriate level of skill and understanding of the Commonwealth's network security legislative and guidance framework for Commonwealth and industry personnel.

4. Deficiencies of the Commonwealth Network Security Guidance Framework

4.1 These observations are derived from Optus' experience of managing electronic information on behalf of the Commonwealth and reflect the current security framework it works within.

Security Standards

4.2 There is currently a lack of consistency in IT security standards between Commonwealth, State and Territory Governments and private industry.

4.3 As a result, private industry faces significant challenges in meeting the security requirements of government. This is particularly noticeable in the areas of security clearances and general IT&T system security.

4.4 There is some mapping between Commonwealth Government guidelines such as the Attorney Generals Department's Protective Security Manual (PSM) and the DSD Security Guidelines for Australian Government IT Systems (ACSI 33) to the more commercial AS/NZS ISO/IEC 17799 standard.

4.5 However there is no clear migration path nor upgrade process for an organisation that meets AS/NZS ISO/IEC 17799 standard to meet Commonwealth government requirements.

4.6 State and Territory Governments are increasingly becoming security conscious, but there is no consistent standard within these organisations and they may use the above mentioned Commonwealth guidelines and commercial standards as necessary to meet their objectives.

4.7 Telecommunications infrastructure is a key part of the national information infrastructure; however there is no recognised security standards mandated for telecommunications facilities and carriage of information.

4.8 As a result, information is protected at different levels depending on which carrier is handling the information.

4.9 Commonwealth departments normally rely on security vetting performed by Defence Security Agency (DSA) and the Attorney Generals Department's Australian Security Vetting Service (ASVS).

4.10 State and Territory Governments rely on police checks and private industry on reference checks. If a private organisation has a Commonwealth contract it can have DSA or ASVS checks performed by the sponsoring agency and these are normally subject to cost and time imposts.

4.11 The current AS/NZS ISO/IEC 17799 standard should be used as a starting point for the development of a graded standard that can be applied to organisations that handle Commonwealth derived and personal information.

4.12 The AS/NZS ISO/IEC 17799:2000 is a risk management code of practice framework for information systems security.

4.13 The standard specifies requirements for establishing, implementing and documenting information security management systems. It is a comprehensive set of defined risks and controls comprising of best practices for effective security management for inter departmental and/or inter organisational dealings.

4.14 Private organisations can then start to put in place a system and security culture that can be more easily upgraded to meet Commonwealth (or State) Government requirements.

Commonwealth Endorsed Products

4.15 Government agencies are currently mandated to use products which have been listed on the Evaluated Products List (EPL) administered by DSD.

4.16 The process of getting a product listed on the EPL is expensive and time consuming and is encumbered by the high turnover of staff within the relevant area of DSD. This factor also introduces a risk to intellectual property, as staff often leave DSD to work for competing private organisations.

4.17 Optus believes that this system should be less complex, less expensive and be faster to complete. This could be an additional system or as an adjunct to the Australian Information Security Evaluation Program administered by DSD.

4.18 Optus also supports the development of a more efficient system to evaluate products and services to determine their security rating and suitability for protection of lower classified and personal information.

Commercial Grade Security for General Government Business

4.19 Due to the requirement to use products listed on the DSD EPL, agencies are not always able to use the security implementations and products that are available commercially, even if they may be more than suitable.

4.20 Optus understands that the value of the information that the Commonwealth has to protect varies widely.

4.21 There are currently two levels of security classification, National Security and Non- National Security.

4.22 The Commonwealth should consider adding an additional level of security classification for the treatment of personal information currently classified under the non-national security classification.

4.23 This amendment would allow the security classification system to include up to date commercial products not contained on the EPL, but sufficient for the treatment of personal information.

4.24 This amendment would also allow the Commonwealth to achieve better value for money without compromising the integrity of the electronic information.

Security Classification Methodology

4.25 Security classification methodology influences all parts of an agencies effort to manage information. Incorrect or over classification of information can lead to unnecessary costs for both the Commonwealth and carriers.

4.26 Incorrect and over classified information led to unnecessary costs for both the Commonwealth and Optus when Optus' was recently contracted to provide Managed IP Network Services (MINS) to the Health Insurance Commission (HIC).

4.27 The Attorney Generals Department's Protective Security Manual (PSM) was used to classify information to be carried on the HIC network.

4.28 The problem is that the PSM guidelines should, but do not classify information using the following criteria.

- value of the information being protected.
- efforts the attacker must undertake to compromise the information; and
- additional costs associated with encrypting 'over classified' information.

HIC MINS Scenario

4.29 The HIC classified its network as 'Protected'. This is likely to be the correct classification based on current guidelines published in the PSM and Australian Communications-Electronic Security Instruction 33 (ACSI 33).

Compromising the MINS

4.30 The MINS will be carried over a private network provided by Optus and will not be carried over the internet.

4.31 The current guidelines do not differentiate between the internet and a carrier provided private network. Both networks are viewed as untrusted, despite the common understanding that the internet has a significantly higher degree of risk than a private carrier network.

4.32 As a result all information carried on the HIC MINS requires encryption because leading to additional costs.

4.33 The current guidelines on classification of information do not take into account what an attacker must go through in order to compromise the information being carried on the MINS.

4.34 This has lead to the implementation of excessive countermeasures to protect information carried on the HIC MINS network.

4.35 The security classification assumes that any HIC premises has appropriate security measures and if an attacker wishes to intercept any information being carried on the MINS, it must be performed outside the secured HIC premises.

4.36 This implies that the carrier has the potential to intercept the information and the attacker has to be an engineer employed by Optus and able to specifically identify and target a telecommunications service amongst all the services that Optus provides and then do something with it.

4.37 The effort required for an attacker to obtain information is significant. If the attacker were able to tap and intercept a MINS telecommunications circuit, all that person would obtain is a raw digital stream.

4.38 The attacker must then have the tools and expertise to analyse the protocols that are running on that circuit and then identify a particular information flow that is of interest to the attacker amongst all the irrelevant and uninteresting information. This processes requires a high level of sophistication and a great deal of time.

4.39 The HIC MINS is a digital data stream, and to identify and tap this data stream and then fully analyse and filter that stream to obtain any useful information is extraordinarily difficult to do.

Value of Information

4.40 After overcoming all the obstacles that the attacker is faced with, the value of information that the attacker may have is highly disproportionate to resources that the attacker would require to intercept and analyse the information.

4.41 A typical example of the type of information obtained from the HIC would be the details of a Medicare claim.

Secure Management Facility

4.42 The HIC was not able to use Optus' carrier grade security controls and procedures as the Commonwealth does not view Optus' security controls and procedures as appropriate.

4.43 As a consequence the MINS had to include an accredited T4 secure facility to manage the MINS that used EPL endorsed products. This all added to the costs incurred by the HIC with questionable benefit.

Classifying Information to the Highest Level

4.44 Optus' experience suggests classifying all information to the highest level is problematic.

4.45 Agencies tend to classify the network to the highest level of classified data that might be carried over it, even if it is only a minor component. This is because agencies find it easer to have one security classification for all information rather than implement the policies, procedures, training and infrastructure needed to manage multiple security classifications.

4.46 Over classifying information and classifying all information at the highest level means that additional countermeasures must be put in place ultimately resulting in higher cost for questionable benefit.