DEFENCE

Defence Signals Directorate
Locked Bag 5076
KINGSTON ACT 2604

Ph: +61 2 6265-0334
Fax: +61 2 6265-0475

DSD 2002/1734
DIR 131/03

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

Dear Mr Catchpole,

ADDITIONAL BRIEFING MATERIAL - INQUIRY into the management and integrity of electronic information in the Commonwealth

I undertook during the Directorate's private briefing to the Committee in March to provide some additional information relating to our role in export controls and the effect of viruses, and also offered a more general background paper of DSD's Information security role.

Attached please find these three papers, release of which has been approved by the Minister for Defence. I am also providing electronic copies separately via email.

If you require any additional information aor clarification, please let me know. My point of contact for this inquiry is Mr Tim Burmeister who can be reached on 02 6265-0323.

Yours sincerely

Stephen Merchant
Director

May 2003

Enclosures:

1. **Effects Of Some Common Viruses On Commonwealth IT Networks**
2. **DSD's role in the Australian Export Control process**
3. **Background Paper On DSD's Infosec Role**

Cc: Depsec Intelligence and Security
Inspector-General of Defence
Assistant Secretary, Ministerial Support and Defence Governance

DEFENCE

Defence Signals Directorate
Locked Bag 5076
KINGSTON ACT 2604

DSD'S INFOSEC ACTIVITIES – A BACKGROUND PAPER

This paper originally represented the DSD input to the written Department of Defence submission to the Joint Committee of Public Accounts and Audit inquiry into the *Management and Integrity of Electronic Information in the Commonwealth*.

> **Terms of Reference**
>
> The Committee shall inquire into and report on the potential risks concerning the management and integrity of the Commonwealth's electronic information.
>
> The Commonwealth collects, processes and stores a large amount of private and confidential data about Australians. Various Commonwealth agencies and private bodies acting on behalf of the Commonwealth hold this information. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrelink keeps social security, family and health information. The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.
>
> In conducting its inquiry the Committee will consider:
>
> - the privacy, confidentiality and integrity of the Commonwealth's electronic data;
> - the management and security of electronic information transmitted by Commonwealth agencies;
> - the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks; and
> - the adequacy of the current legislative and guidance frameworks.

The Defence Signals Directorate (DSD), located within the Department of Defence, is the national communications and computer security advisory authority. DSD is responsible for providing advice and assistance to Commonwealth and State agencies about protective security policy and procedures in communications and information technology.

1. The privacy, confidentiality and integrity of the Commonwealth's electronic data
2. The management and security of electronic information transmitted by Commonwealth agencies
3. The management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks

DSD provides advice and assistance on information security - including confidentiality, integrity, availability, authenticity and non-repudiation - to Australian Commonwealth and State agencies. Advice and assistance is available across a range of areas:

- *Government Security* – DSD provides advice and assistance to Australian Commonwealth and State agencies and their commercial IT security service providers to promote understanding and implementation of the relevant Commonwealth information security policies. Activities include developing security guidelines and policy, performing Internet gateway reviews, conducting security audits, conducting information security training and convening relevant information sharing fora.

- *IT Security Product Evaluation* – The Australasian Information Security Evaluation Program (AISEP) provides a mechanism for assessing the level of assurance that can be placed on the security claims made for commercial IT security products. Impartial companies (known as Australasian Information Security Evaluation Facilities) perform evaluations under the program, against internationally recognised standards and criteria. The results of these evaluations are certified by DSD as having rigorously followed the standards in all aspects.

- *Government Projects* – DSD provides assessment of the IT security framework of Commonwealth wide e-business and e-security projects, and works with the National Office for the Information Economy to ensure security of the Commonwealth government's *Gatekeeper* project.

- *Communications Security policy* – DSD provides national doctrine and policy on the provision of secure communications services to the Department of Defence and other Government organisations.

- *Cryptographic support* – DSD provides advice and assistance in acquiring High Grade Cryptographic Equipment to the Department of Defence and other government organisations.

- *Cryptographic production, distribution and management* – DSD produces, distributes and manages cryptographic key material for the Department of Defence and other government organisations.

- *Computer Network Vulnerability* – DSD investigates attacks against government and National Information Infrastructure (NII) computer related assets. In addition, DSD also research security vulnerabilities and provides reports and presentations to educate customers regarding information security issues.

- *Incident reporting* – DSD has established an incident reporting scheme (ISIDRAS) to collect information on security incidents which affect the security or functionality of Commonwealth computer and communication systems.

For example, DSD provided assistance to the Australian National Audit Office last year in its audit of Internet security of Commonwealth agencies. DSD acted as technical adviser, contributing the technical knowledge required in order to complete the audit and test the security of selected Internet sites. Results of this audit can be found in The Auditor-General Audit Report No. 13 2001-2002 Performance Audit *Internet Security within Commonwealth Government Agencies*. In summary, the level of security afforded by agencies to their Internet presences ranged from very good to very poor, resulting in a number of specific recommendations aimed at resolving the security issues identified. The report also found that agency management of Internet security was broadly consistent with the provisions of both the *Commonwealth Protective Service Manual* and DSD's *Australian Communications – Electronic Security Instruction 33* (ACSI-33).

Generally speaking, DSD has found that the management and security of the Commonwealth's electronic information is quite variable – the results of the ANAO audit being indicative of the varying levels of information security found throughout Commonwealth agencies. For systems containing National Security Classified material the standards set are well defined and quite rigorous in their application. It is generally more difficult to protect information systems carrying Non-Nationally Classified material, as there is greater scope in the security guidelines for individual agencies to manage the risks appropriate to their environment.

4. *Current legislative and guidance frameworks*

The *Intelligence Services Act 2001* outlines DSD's role as the national authority on information security as follows:

> S7. The functions of DSD are:
> (c) to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processes, stored or communicated by electronic or similar means; and
> (d) to provide assistance to Commonwealth and State authorities in relation to cryptography and communications technologies.

Commonwealth Government agencies are required by the *Commonwealth Protective Security Manual* (PSM) to consider the security implications of their electronic information systems and to devise policy and plans to ensure the systems are appropriately protected. As part of DSD's national information security role, the Directorate produces a range of documents that provide standards and guidance for Commonwealth agency computer and communications systems. The main publications are as follows:

- *Australian Communications-Electronic Security Instruction (ACSI) 33-Security Guidelines for Australian Government IT Systems*
  ACSI 33 has been developed by DSD to provide guidance to Australian Government agencies in protecting their information systems. It discusses the security issues for all Commonwealth Government electronic information systems, whether they process classified information or other critical but unclassified information, and regardless of whether they are a large or small, multi-user or single-user system.
- *Supplement No. 1 to Australian Sigint Security Regulations and Orders (ASSRO Supp 1) - Security Standards for Sigint Computer Systems*
  ASSRO Supp 1 details the security requirements for any computer system which handles or may have access to Sigint (SI) material. It is issued by the authority of the Secretary, Department of Defence, who is responsible for the overall security of SI activities in Australia. Observance of the requirements and procedures detailed in this publication is mandatory for all Australian organisations or individuals authorised by the Secretary for Defence, to collect, produce, receive, process, communicate or store SI material or information.

- *Gateway Certification Guide*
  The Gateway Certification Guide provides agencies seeking DSD certification of their gateway facility with details of the requirements that they must fulfil to achieve certification. DSD gateway certification is a voluntary process which aims to provide Commonwealth agencies with an independent assessment that their gateway has been configured and managed to industry best practice.

DSD also produces a range of more specific instructions relating to specific aspects of communications and information technology security. DSD considers its publications provide an adequate guidance framework for Commonwealth agencies. However, they are currently being reviewed to update their content particularly in light of new and emerging technologies. *ACSI 33* and *ASSRO Supp 1* for example are planned for revision in July 2003.

As part of this review process, DSD is also considering developing *ACSI 33* to ensure that it clearly details mandatory minimum information security requirements for government systems. This will make it easier for agencies to meet the *Commonwealth Protective Security Manual* requirement for agencies to meet the “minimum standards of *ACSI 33*”. Additionally, DSD plans to review the standards for National Security Classified material below TOP SECRET.

DEFENCE

Defence Signals Directorate
Locked Bag 5076
KINGSTON ACT 2604

Ph: +61 2 6265-0334
Fax: +61 2 6265-0475

DSD'S ROLE IN THE AUSTRALIAN EXPORT CONTROL PROCESS

Background

Australia is a signatory to the Wassenaar Arrangement , which helps form Part 3 (Dual-use goods and technology) of the Australian Defence Strategic Goods List (DSGL), administered by the Defence Trade Control & Compliance (DTCC) section in the Defence Materiel Organisation.
Part 3 of the Strategic Goods List has nine categories The fifth category relates to Telecommunications and Information Security. DSD provides expert technical advice to the Trade Control and Compliance Section on any export applications involving category five goods, since these goods generally use cryptography.
DSD provides the Trade Control and Compliance Section with Assessment sheets, which make recommendations about whether an export license should be granted, and includes any associated conditions of use to be placed on the exporter (e.g. quarterly report on the number of sales including names and addresses of end-users).
The Australian export control regime for cryptographic products is generally similar to that maintained by other Wassenaar Arrangement signatories, such as the United Kingdom and the United States. It is the national delegates to the Arrangement who determine and agree (by consensus) on the detail of control parameters to be applied (including matters such as key length for cryptography). These parameters form the basis of the national policy of individual member nations.
Australia's involvement in the Arrangement, and DSD's role, is to ensure that Australian industry is able to develop cryptographic products for export while managing possible threats to Australia's national security.

export application approval

The decision-making process includes assessing the cryptography used in the product to be exported, and determining if it is listed on the Strategic Goods List, under part three category five, as a controlled item.

- DSD identifies the cryptographic algorithm or function being used in the product, and the relevant control status. For example;

  - symmetric algorithms using key lengths greater than 56 bits in length are controlled (some examples include DES, 3DES and AES).

  - Asymmetric algorithms are controlled where the security is in the factorisation or computation of discrete logarithms greater than 512 bits (some examples include RSA, Diffie-Hellman, DSA).

- If the item is controlled, DSD, in consultation with relevant areas of the Defence Organisation, assesses whether the export may affect Australia's national security or strategic defence capability.

- If it is controlled, and the export does in some way affect Australia's national security or strategic capability, then, unless the company withdraws the application voluntarily, DSD would recommend to Trade Control and Compliance Section that the export application be denied.

- The Minister for Defence, is the only member of the Australian Government empowered to make this decision. The Minister would require substantial evidence regarding the detrimental effect export approval would have on Australia's national security or strategic capability, prior to giving his approval.

- This information would only be presented to the Minister for Defence after a special meeting of the Defence Materiel Cooperation Export Committee, or the Standing Inter-Departmental Committee on Defence Exports.

- If the product is controlled and the export does NOT affect Australia's national security or strategic capability, DSD makes a recommendation about the type of license to be granted is. This recommendation takes into account the intended purpose of user, and the identity of the end-user.

    - ♦ For Government/Military end-users there is a requirement to have a "statement by ultimate consignee" form filled out, before the export can be processed.

    - ♦ For non-government/military users a general export license is granted that requires post-sales reporting to be submitted to Defence on a quarterly basis.

- More information can be found on the DMO website under the *Defence and Strategic Export Controls* section at the address:

  www.defence.gov.au/dmo/DMO/export_controls.cfm

Defence Signals Directorate
Locked Bag 5076
KINGSTON ACT 2604

EFFECT OF SOME COMMON VIRUSES ON COMMONWEALTH IT NETWORKS

Background

This paper collates information reported via the Defence Signal Directorate's Information Security Incident Detection, Analysis and Reporting Scheme (ISIDRAS). The Protective Security Manual stipulates that agencies must report significant incidents. Many of the reports are generated as a result of DSD contacting the agency concerned, and consequently the picture it provides is an indicative one. DSD is encouraging use of the scheme, including a 24-hour incident response service, through its Computer Network Vulnerability Team.

Discussion

Since January 2001, approximately 30% of reports to ISIDRAS (excluding port scanning reports) have been virus or Internet worm incidents. The overall effect on Australian Government systems has been minor (especially when compared with statistics gathered by various anti-virus vendors from the Internet as a whole).

Based on ISIDRAS reporting each of the major virus/worm infections that have infected the Internet have affected Australian Government Systems to varying degrees. The effects have ranged from the infection of a number of machines on an internal network to one or two machines only being infected. Other effects have been the closure of gateways by Agencies while security staff assess the Agency's vulnerability to a particular threat.

Statistics report only infections or consequences and do not report the effort involved to determine system vulnerability and to take appropriate preventative measures. DSD informally surveyed many agencies after the *BugBear* and *Slammer* events and learned that a significant effort was made to mitigate the effects of the two worms as they propagated on the wider Internet over and above any effort made to clean up systems that had actually been infected.

Summary of reports received

- Slammer (January 2003). No reported infections. Some reports of a Denial of Internet service because of the worm's activity.

- BugBear (October 2002). Five agencies reported infection. One agency was re-infected after cleanup.

- MyLife (April 2002). Three agencies infected, reported by gateway service provider

- MyParty (January 2002). Three agencies infected, reported by gateway service provider

- Goner (December 2001) Four infections reported

- Nimda (September 2001) Four infections

- Code Red (July 2001) Five infections

Causes of infection

- infection occurs before Anti-virus updates received or implemented

- staff introducing viruses by bringing in media, ie floppy disks, CDs etc. (lack of user education)

- inadequate patching regime (Nimda on internal servers)

- inadequate clean up (Nimda through Code Red hole)