02 6234 1218

Australian Security Intelligence Organisation

Submission to the Joint Committee of Public Accounts and Audit

"Inquiry into the management and integrity of electronic information in the Commonwealth"

15 October 2003

ASIO's role in the protection of electronic information

ASIO's role with regard to the protection of classified material in the Commonwealth, including electronic information, is primarily an advisory one.

ASIO's role is defined in paragraph 17(1)(d) of the *Australian Security Intelligence Organisation Act* of 1979 (the ASIO Act) which states that a function of the Organisation is to provide advice to Ministers and authorities of the Commonwealth on matters relating to protective security. The provision also states that advice can be given to such other persons as the Attorney-General, by notice in writing to the Director-General, determines.

In practical terms ASIO provides advice and assistance, on request, to Commonwealth agencies or other organisations about protective security measures that can help safeguard national security classified information.

The responsibility for the security of individual agencies and departments rests with Agency Heads.

Agencies are not required to seek ASIO advice in relation to sites holding or using information classified below Top Secret level. However, many agencies choose to employ ASIO to provide advice on their physical security measures and/or certify their sites. This service is provided by ASIO on a cost recovery basis in accordance with a Government decision.

Relevant standards

ASIO's advice on the protection of electronic information in the Commonwealth is provided in accordance with the following Commonwealth publications and standards:

- The *Commonwealth Protective Security Manual 2000* (the PSM).
- The Defence Signals Directorate *Australian Communications – Electronic Security Instruction 33 - Security Guideline for Australian IT Systems, Handbook 14* (ACSI 33).
- The Defence Signals Directorate *Australian Sigint Security Regulations and Orders Supplement 1 Part A – Security Standards for SI Computer Systems* (ASSRO Supplement).

ASIO's advice addresses such issues as:

- Physical barriers such as doors, windows, walls, floors and roofs,
- Locks and other door hardware,
- Security alarm systems and appropriate responses to alarms,

- Electronic access control,
- Security grills for air conditioning ducts, and other penetrations in the perimeter of the area, and
- Procedural measures to ensure the correct operation of the physical security measures.

Physical security requirements

The appropriate physical security standards for IT systems (including communications equipment, servers, and workstations) are defined in the DSD publications, ACSI 33, ACSI 37, and the ASSRO supplements.

The physical security requirements for a server room or workstation will vary depending on the classification of the information involved, and the environment in which the equipment is located. Depending upon the environment in which an agency is operating, these requirements may include different grades of areas, and the use of appropriate security containers.

The physical security for an IT facility generally consists of an Intruder Resistant or Secure Area perimeter enclosing the entire user network, a more restrictive area separated from general user areas containing the servers and communications equipment, and the protection of the facility by appropriate physical security measures to limit access to those with the authorisation and requirement to enter, and to detect those attempting to gain unauthorised access.

Depending upon the classification of the information it contains, a server room containing communications and server equipment is required to meet either the Intruder Resistant or Secure Area requirements.

Up to and including Secret information

Areas containing networks handling information up to and including Secret information are required to meet the minimum standards for an Intruder Resistant Area, as defined in the PSM as:

- Tamper-evident barriers, resistant to covert entry, and
- An effective means of limiting entry to authorised people only during both operational and non-operational hours.

Top Secret information

The PSM assigns responsibility for the certification of overall physical security measures for Top Secret facilities to ASIO. Certification is required prior to first use, after significant structural or equipment alterations, and at least every five years thereafter.

ASIO's certification forms part of DSD's accreditation of Top Secret sites.

Agencies are required to have the measures certified by ASIO in accordance with the relevant standards set out in the PSM and ASSRO Supplements. Areas containing networks handling information up to and including the level of Top Secret are required to meet the standards for a Secure Area as defined in the PSM as:

- Appropriately secured points of entry and other openings,
- A tamper-evident barrier, highly resistant to covert entry,
- An effective means of limiting entry to authorised people only,
- All staff requiring frequent entry must hold an appropriate security clearance,
- All visitors and contractors are to be escorted at all times,
- All staff are to display their passes while in the area, and
- A Type 1 Security Alarm System (SAS) or ASIO-approved security alarm system for site-specific applications, or appropriately trained and cleared on-site guards conducting internal patrols to physically check each security container at intervals not exceeding 120 minutes.

Server rooms containing Top Secret communications and server equipment are also required to meet the Secure Area requirements.

ASIO has also developed detailed guidelines that are intended to assist departments and agencies to develop an appropriate physical security environment for Top Secret material that will satisfy the relevant guidelines and standards.