3

Physical Security

3.1 The second term of the Committee’s review addressed the physical security arrangements in place in each of the agencies. For the purposes of the review, the Committee defined physical security as: that part of protective security concerned with the provision and maintenance of a safe and secure environment for the protection of agency employees and clients, and physical measures designed to prevent unauthorised access to official resources and to detect and respond to intruders.

3.2 The Committee’s first interest was to obtain an overview of the physical security controls and procedures applied by the agencies in accordance with the Commonwealth’s Protective Security Manual (PSM), and in particular the PSM’s guidelines for the protection of security classified information and assets. The Committee was also interested in assessing progress by the agencies in implementing the recommendations of the IGIS Inquiry relating to physical security.

3.3 The Committee briefly considered the requirements of the PSM, some of the key physical security controls and procedures maintained by the agencies - including measures recommended by the IGIS Inquiry – and mechanisms for reviewing security arrangements.

3.4 In general, the Committee found that the physical security regimes maintained by each of the three agencies met, and in many areas exceeded, the standards set out in the PSM. It was also evident that many of the physical security measures recommended in the IGIS Inquiry were already in place, or required only minor modification to ensure compliance. The agencies demonstrated that they were also making substantial progress in addressing the remaining recommendations of the IGIS Inquiry.

3.5 The Committee identified a number of areas of physical security where more work needs to be done. This includes the development of new controls and procedures for regulating access to shared-use office equipment, improving capacity to meaningfully analyse audit information obtained. The Committee acknowledges that work in these areas, particularly with regard to the development of technological solutions, will take time.

Physical Security Requirements

3.6 The PSM emphasises that physical security is an essential element of an agency's total protective security framework. Physical security measures provides the first line of defence against intrusion or attack, and the most visible form of deterrence against unauthorised removal of information and assets. Physical security also provides an important support to other personnel and administrative security measures.

3.7 Part E of the Protective Security Manual (PSM) details the Commonwealth's requirements for creating and maintaining an appropriate physical security environment for the protection of official information and resources, and for employees and clients. The PSM does not proscribe a common standard of treatment that should apply to all installations and establishments. Rather, it provides guidance to agencies on determining the appropriate level of physical protection for their functions and official resources, and controls that they can utilise to treat security risks.

3.8 The PSM does provide more specific advice, in the form of common minimum standards, for the protection of security classified information. These standards apply to the handling and storage procedures for security classified information, logical controls for IT systems carrying such information, personnel security requirements, and physical barriers to control access[1]. For ASIO, ASIS and DSD, these standards form the basis of their physical security regimes.

3.9 The IGIS Inquiry advocated a number of additional measures for AIC agencies in relation to physical security, which essentially build on

[1] Attorney-General's Department, PSM, Part E, paragraph 4.13.

the standards established by the PSM. In some areas, this involved agencies modifying existing systems and procedures. In other cases, it also required agencies to consider the development and application of new measures, particularly with respect to entry controls and security features for office equipment.

Physical Security Measures

3.10 As agencies that process and handle the highest level of security classified information, ASIO, ASIS and DSD are required to maintain a range of physical security measures that meet, as a minimum, the standards set out in the PSM for the protection of security classified information and resources. Importantly, each of the three agencies confirmed that the physical security regimes they maintain at their facilities (including offices and other installations) exceed the requirements of the PSM.

3.11 The Committee did not take detailed evidence on all physical security measures utilised by the agencies (for example, on various types of security hardware) to protect official information, employees and clients. Rather, it focused on a number of controls identified by the IGIS Inquiry and by the agencies themselves in their formal submissions.

Entry Controls

3.12 Each of the agencies employs a range of controls to limit physical access to premises and work areas housing security-classified information. These include electronic controls, physical barriers, human controls (such as a guard presence) and administrative procedures.

3.13 The IGIS Inquiry recommended that AIC agencies consider the introduction of turnstile-type systems and/or biometric recognition when upgrading systems for controlling entry and exit to secure premises. This would further reduce the scope for “piggybacking” and improve the capture of traffic information for audit purposes.

3.14 ASIO reported that it currently utilises an electronic control access system to positively identify personnel entering and leaving ASIO Central Office (ACO) and its largest state offices. This system enables ASIO to electronically log and audit information on all staff movement into and out of these premises. ASIO noted that the electronic access system would be extended to other state offices by the end of 2002. ASIO said that further study and trialling of biometric access controls was required before a decision was made on introduction.

3.15 ASIS told the Committee that it was satisfied that the access control mechanisms in place at its facilities met the requirements of the PSM, and adequately addressed the needs, identified by the IGIS Inquiry, to restrict unauthorised access and provide for full audit of traffic. ASIS stated that it had no plans to introduce biometric technology to its access control system at this stage, but would assess biometric applications employed by other AIC agencies before considering implementation.

3.16 DSD has commenced work on upgrading access controls at its headquarters facility. The upgrade will provide for a single entry and exit control mechanism combining biometric recognition and identification card. The upgrade will also provide for increased control on movement to and from certain compartmented areas within DSD's headquarters facility. At other sites, DSD utilises conventional physical barriers, identification passes and guards to control entry and exit.

3.17 The Committee considers that the entry controls that each of the agencies currently has in place are fit for purpose and adequately meet the requirements of the PSM. The Committee agrees with the decision by ASIO and ASIS to defer implementation of biometric access controls until further trialling and evaluation of available and cost-appropriate options has been undertaken. Ideally, agencies should seek to develop a single biometric-based access control that can be used for physical access and access to secure IT networks.

Alarm and Surveillance Systems

3.18 Each of the agencies utilise intruder alarm systems at offices and other facilities to protect secure areas, as required by the PSM. These systems are primarily used to support, rather than replace, site guards in maintaining security, and also serve as the primary form of intruder detection during non-operational hours.

3.19 ASIO reported that it had upgraded the various electronic security systems deployed at its offices. ASIS provided few details on its alarm and surveillance systems, but confirmed that all ASIS locations have the physical security controls required to protect security classified information at the TOP SECRET level. DSD reported that it planned to complete the upgrade of its Electronic Intruder Detection System (EIDS) Type 1 alarm by the end of 2002. This will provide for auditable tracking of entry and movement throughout DSD premises, and enable DSD to further restrict access to sensitive areas within DSD sites.

3.20 The Committee did not take enough evidence on alarm and surveillance systems used by the agencies to draw any conclusions, other than to note that the agencies have taken steps to ensure that they can generate auditable information on access to and movement within all secure areas.

Security Guards and Attendants

3.21 Each of the agencies utilise guard forces and security attendants as critical components of their physical security regimes. They conduct entry control procedures (for example, pass checking) and escorting visitors, monitoring intruder alarm and surveillance systems (such as close circuited television) and conduct internal and external patrols.

3.22 ASIO maintains an in-house security attendant staff at each of its Australian offices. ASIS also utilises in-house security staff to manage entry and exit control procedures. DSD's guard contingent at its headquarters facility is provided by the Defence Security Authority. At other locations, DSD employs guards from the Australian Protective Security Service.

3.23 The Committee considers that the current use by agencies of security guards and attendants as part of their protective security framework is appropriate, and consistent with the "security-in-depth" approach advocated by the PSM. However, as new technologies are introduced to further automate physical security systems, agencies should identify and take advantage of opportunities to reduce reliance on the use of guards and attendants.

Entry and Exit Searches

3.24 An important element of an effective access control system is the capacity to control not just the movement of people, but materials into and out of secure areas. The use of personal and baggage searches, administered by security attendants or guards, can guard against the transport of unauthorised electronic recording and transmitting equipment, copying equipment or explosive devices into secure areas. Similarly, exit searches can act as a deterrent to the unauthorised removal of resources, especially security classified information.

3.25 The PSM provides for the consideration by agencies of the use of entry and exit searches, but encouraged agencies to consider other security measures first. The IGIS Inquiry, addressing the special security environment of the Australian Intelligence Community, recommended that AIC agencies require random baggage searches as a condition of entry and exit to premises.

3.26 In evidence to the Committee, ASIO noted that it had established arrangements for conducting random bag searches at its Central and State offices following the Cook Inquiry in 1994. ASIS reported that it conducts random bag searches at its headquarters facility, and has done so for some time. Neither agency reported any negative feedback from staff about its search procedures.

3.27 DSD informed the Committee that, under the Crimes Act, it was not legally permitted to enforce random bag searches at its headquarters facility in Canberra. DSD indicated that it had initiated steps to have the Northgate compound (which includes DSD headquarters) declared "prohibited place" under the Crimes Act, and that this would provide a legal basis on which to conduct and enforce searches.

3.28 The Committee strongly supports the use by agencies of entry and exit searches as part of their access control regimes. Such practise should be based on documented procedures, which are made available to all staff and visitors to those sites where searches are carried out.

3.29 With regard to DSD, the Committee recommends that :

Recommendation 3

That, as a priority, DSD implement random bag inspection procedures at all its headquarters facilities and all other installations in Australia.

Electronic Article Surveillance

3.30 The PSM 2000 does not require agencies to use electronic article surveillance systems (or electronic tagging) to assist in protecting against the unauthorised removal of security-classified information or assets.

3.31 The IGIS Inquiry recommended that agencies which did not have electronic article surveillance systems in place evaluate them for possible introduction at entry and exit points.

3.32 In response, AIC agencies tasked the IASF's Personnel and Administrative Security Working Group to study the applicability and effectiveness of electronic tagging, and develop recommendations on possible implementation. At the time of writing, this matter was still under consideration by the IASF. ASIS noted that it had installed electronic tagging and detection units at its headquarters facility, but provided no details on its procedures.

3.33 The Committee considers that electronic article surveillance systems should be a standard physical security measure for AIC agencies. Electronic tagging should enhance agency capacity to accurately detect and track the transport of sensitive materials to and from secure areas, and provide an additional deterrent to unauthorised removal of security classified assets.

Recommendation 4

The Committee recommends that, subject to the outcomes of the IASF working group findings, ASIO, ASIS and DSD allocate funding for the development and implementation of electronic article surveillance systems for all Australian offices and installations.

Management of Classified Material

3.34 The terms of the review did not address agency management of information security specifically, but did consider certain aspects of the management of classified information and protection of electronic information.

3.35 Part C of the PSM details the Commonwealth's procedures for the handling and storage of security classified information. It requires agencies, inter alia, to maintain a register for security classified documents, file and store information in appropriate containers, and establish procedures to account for security classified documents at all times.

3.36 The IGIS Inquiry recommended that AIC agencies audit their compliance with the PSM's procedures for information and file handling, and also conduct a full muster of accountable documents.

3.37 ASIS noted that it participated in the IASF's one month trial muster of accountable documents in 2002, and that the muster produced no unaccountable documents. ASIS indicated further that it had instituted quarterly audits of accountable documents to comply with the recommendations of the IGIS Inquiry.

3.38 DSD reports that it conducts a file census annually, which involves identification of all files and their present location. DSD also records all file movements in a database, which has the capacity to track the last five locations of each file. DSD did not comment on whether it had conducted a trial muster of accountable documents in the past twelve months.

Office Equipment Security

3.39 Part C of the PSM 2000 deals with procedures for protecting security classified information, including general advice in relation to the use of office equipment to print, copy or transmit security-classified information.

3.40 The IGIS Inquiry made a number of more specific recommendations on improving the security controls that agencies apply to their office equipment. These include upgrading equipment to include security features (such as user identification and audit functions), and additional procedures to restrict access to equipment to authorised users.

3.41 ASIO reported that IASF's Information Management Working Group was examining the implementation of security features for photocopiers, facsimiles and printers, and that some IASF agencies had already implemented security features for their equipment. ASIO said it was in the process of trialling applications used by other agencies as well as other commercially available technologies to determine the most appropriate solution for its security needs.

3.42 ASIS and DSD have both developed in-house projects to review the use and accessibility of photocopier and facsimile units, and to evaluate options for upgrading equipment to meet security requirements identified by the PSM and the IGIS Inquiry.

3.43 ASIS told the Committee that it had completed the first phase of the project – identifying all equipment and its business need – and was now working with a commercial vendor on a technological solution to enable ASIS to capture as much information as possible on copying and faxing activities. ASIS said it was also working on updating its policies and procedures for the use of copiers and faxes within the organisation.

3.44 DSD reported that it had reviewed its arrangements for use and access to photocopiers and facsimile machines, and that these satisfied the requirements of the IGIS Inquiry. It had also undertaken evaluation of advanced security features for its photocopy units. Once evaluation was complete, existing units would be completed on a priority-needs basis.

3.45 The Committee notes that each of the agencies has reviewed its policy and procedures regarding the provision and use of photocopiers and facsimile machines, and taken steps to limit access to such equipment to authorised users in designated work areas. The Committee considers that agencies should, if they haven't done so already, develop and document interim procedures for the continued use of non-secure equipment.

3.46 The Committee accepts that the upgrading of office equipment to include security features recommended by the IGIS Inquiry depends to large extent on the availability of appropriate technology, and the resources to acquire and install that technology in the work place. The Committee encourages agencies to take steps to ensure that the upgrading of equipment causes minimal disruption to operational activities.

Protection of Employees

3.47 The Committee's review focused primarily on physical security measures designed to prevent unauthorised access to secure areas, and unauthorised removal or disclosure of security classified information and other official resources. However, it is important to emphasise that the physical security arrangements in place in each of the agencies are also intended to provide a high standard of protection for employees and clients.

3.48 The PSM requires agencies to provide a safe physical security environment for employees for two reasons. Second, the Commonwealth has a responsibility to protect its most valuable resources: the knowledge, skills and capabilities of its employees. This responsibility is particularly important for agencies such as ASIO, ASIS and DSD, where personnel are potentially vulnerable to harm because of the nature of their work or their proximity to official resources that may be targeted.

3.49 Many of the physical security measures employed to protect security classified information and other resources also provides protection for employees and clients. For example, the use of access controls that require positive identification of individuals entering secure premises greatly reduces the risk of unauthorised entry. Similarly, a security guard presence serves as a deterrent and improves an agencies capacity to respond to security incidents quickly.

Additional Measures

3.50 In addition to these standard controls, each of the agencies also employs a number of measures that address the specific risks facing personnel working in a highly classified environment. These measures include additional physical layers of security for buildings and installations, and for two of the agencies, use of institutional security (such as operational cover) to protect staff. For the purposes of this report, the Committee focused on additional physical measures, and the issue of co-location.

3.51 ASIO reported that it had made a number of changes to its physical security arrangements to improve protection for staff in the past three years. These included: the installation of security bollards on access roads to ASIO's Central Office (ACO); upgrading various electronic security systems at ACO; and the installation of a secure room and "Glove Box" for opening public mail –protecting staff from potential biological and chemical hazard.

3.52 ASIS and DSD confirmed that they maintained a number of additional physical security controls, such as security fencing and bollards at certain installations, to enhance staff security. Both agencies also indicated that they had conducted comprehensive reviews of physical security arrangements at all premises following the terrorist attacks in the United States on 11 September 2001, and in Bali, Indonesia on 12 October 2002.

3.53 The Committee considers that these additional security measures are extremely important. They serve as a further deterrent to physical attacks on agency property and personnel, and symbolically, provide a visible demonstration of the Commonwealth's commitment to protecting its personnel.

Co-location

3.54 Given the recent increased threat of terrorist attack to Australian government organisations and personnel, the Committee was particularly interested in work by the agencies to address the potential security problems arising from physical co-location of establishments with other government agencies.

3.55 The PSM provides only general guidance to agencies on co-location. It states that where agencies share locations, the protective security measures applied by all the agencies involved must address the collective risks that result from co-location, as well as any specific risks that an agency may face.

3.56 In evidence to the Committee ASIO and ASIS confirmed that they had a number of co-located offices, and that in each case, the agencies had entered into detailed agreements with co-tenants on cooperative security arrangements for those locations. ASIO and ASIS also confirmed that they had reviewed physical security at each of their co-located premises in light of the heightened national security threat level, and had determined that existing security arrangements were appropriate in all but one case affecting ASIO.

3.57 The Committee was satisfied that the agencies had given adequate and timely consideration to physical security at their co-located premises. It noted that remedial work at the one establishment cited had commenced, and would be completed by mid-year.