1

Introduction

1.1 The Parliamentary Joint Committee on ASIO, ASIS and DSD (the Committee) resolved on 27 June 2002 to conduct a private review, under Section 29 (1)(a) of the Intelligence Services Act 2001, of protective security in ASIO, ASIS and DSD. Section 29(1)(a) of the Act provides for the Committee to review administration and expenditure matters of ASIO, ASIS and DSD without reference from a responsible Minister or resolution of either House of the Parliament.

1.2 The terms of the review addressed the agencies' administration of security issues, including the implementation of recommendations arising from the Inspector General of Intelligence and *Security Inquiry into Security Issues* (the IGIS Inquiry), with particular reference to:

- personnel security,
- physical security;
- information technology (IT) security; and
- the adequacy of legislation dealing with espionage crime, including the provisions in the Criminal Code Amendment (Espionage and Related Offences) Bill 2002.

1.3 The Committee invited the three agencies to make submissions to the review addressing the above terms. It also invited a number of other Commonwealth agencies to enter submissions on their security arrangements and views on ways protective security policies and practices can be enhanced.

1.4 The Committee held private hearings in Canberra, in December 2002, and March 2003, at which the three agencies provided evidence. The Committee also took evidence from the Australian Crime Commission (formerly National Crime Authority), the Australian Customs Service (ACS) and the Australian Federal Police at a private hearing in February 2003.

1.5 The Committee invited the Inspector-General of Intelligence and Security (IGIS) to give evidence to the review. IGIS declined to make a formal submission but did agree to give evidence in person. Unfortunately, the Committee was forced to postpone a private hearing with IGIS, scheduled for March 2003.

Background

1.6 The Committee's decision to undertake the review was motivated primarily by an interest in the Commonwealth's response to a number of publicised cases of attempted espionage involving employees of one of Australia's intelligence agencies in 1999 and 2000, and the resulting inquiry by IGIS into improving security within government, which was completed in September 2000 (see below).

1.7 The Committee had a broader interest in the adequacy of protective security arrangements in place in the agencies in the light of the terrorist attacks of 11 September 2001 in the United States, and Australia's continuing role in international efforts to combat terrorism. The Committee's interest in agency security was given further impetus by the terrorist bombings in Bali Indonesia on 12 October 2002, and the assessment by the Australian Government of an increased threat to government property and employees both here and overseas.

1.8 The Committee recognised that the review and refinement of protective security within Australia's intelligence and security agencies is an ongoing process, and one that is accorded a high priority by the Australian Government. It noted that protective security within ASIO and ASIS was significantly enhanced as a result of major government-commissioned inquiries in the 1990's, while DSD's security program has been improved by a number of internal review processes during the same period.

Protective Security Manual

1.9 The Commonwealth's Protective Security Manual (PSM) sets out the practices, policies and procedures that all Commonwealth organisations, are required to follow to establish and maintain an effective protective security environment. It contains guidance to agencies on a range of protective security controls and procedures to protect their official information, assets and human resources from potential security threat and risks.

1.10 The PSM was revised and re-issued, following endorsement by the National Security Committee of Cabinet (NSC), in December 2000. In addition to more comprehensive advice on security controls and procedures available to agencies, the revised PSM also contains a series of minimum standards for the conduct of certain protective security processes.

1.11 The PSM proposes that agencies adopt a risk-based control framework to manage protective security. The proposed framework comprises a number of complementary and supporting measures, which include:

- Personnel security measures (for example, security vetting of staff)
- Physical security measures (for example, physical access controls);
- Administrative security measures (for example, the application of the "Need to Know" principle to classified information)

1.12 The PSM expects that agencies will develop a protective security framework based on a number of general and related principles. These principles include: appropriate restrictions on access to information based on the need to know; the classification and protection of information based on the adverse effects of disclosure; and the integration of security measures to create security-in-depth.

Need to Know Principle

1.13 A key principle underpinning the Commonwealth's protective security policy involves limiting access to official information to those individuals who need to use or access the information to do their work, which is referred to as the need to know principle (NTK).

1.14 All protective security processes within ASIO, ASIS and DSD are premised on the NTK principle. In addition to the use of secure areas, each agency also maintains information management systems and a range of administrative processes to effectively "compartmentalise" and control access to information.

Security Classification

1.15 A second, related principle underpinning the protective security framework proposed by the PSM is that of identifying or classifying official information based on the potential harm caused by its unauthorised disclosure, and the application of appropriate levels of protection to minimise that risk.

1.16 The Commonwealth's security classification system (as detailed in Part C of the PSM) requires all agencies to apply a security classification to official information, where the compromise of that information could cause harm to the nation, to the public interest, the Government or other entities and individuals. It further requires agencies to adopt a range of security controls and procedures (as a minimum) to protect that information according to the level of classification.

Security-in-Depth

1.17 The PSM makes explicit the need for agencies to adopt a combination of security measures to address security risks. This combination of measures is intended to establish a series of barriers, or security-in-depth, to prevent or restrict unauthorised access to official information and resources. For example, agencies might employ a combination of controls to limit entry to their premises, including use of electronic identification cards, security guards or attendants to monitor entry and egress points (and prevent piggybacking) and administrative procedures such as registers and temporary identification passes for visitors.

1.18 As agencies dealing with highly classified resources, ASIO, ASIS and DSD each maintain protective security regimes which operate on the security-in-depth principle. For ASIS, this security-in-depth also includes a layer of institutional security designed to reduce the visibility of routine activities that could lead to a compromise of ASIS operations or its staff.

The IGIS Inquiry into Security Issues

1.19 The Inspector General of Intelligence and Security (IGIS) was commissioned by the Prime Minister to provide advice on measures to be taken by Commonwealth agencies to improve protection of classified information and assets, following the arrest of a former DIO officer, on espionage charges in 1999. The IGIS focussed its inquiry on Commonwealth departments that handle highly classified information and Australia's six intelligence and security agencies, but its findings are also relevant and applicable to other Commonwealth organisations.

1.20 The report of the inquiry, which was presented to the Prime Minister in March 2000, contained over 50 recommendations addressing: management responsibilities for security; inter-agency issues; personnel security practice and procedures; physical security arrangements; and computer security. All the recommendations of the IGIS Inquiry report were endorsed by the Prime Minister and Cabinet, and referred to agencies for implementation.

Review Objectives and Focus

1.21 The Committee's interest in conducting the review was to gain an overview of the protective security arrangements in place in ASIO, ASIS and DSD, and recent work done by the agencies to address security requirements identified by the revised PSM and the IGIS Inquiry. The Committee's intention was not to attempt an exhaustive stock take of each agency's security policies, practices and procedures in relation to the PSM. The Committee considers that its review is no substitute for a comprehensive external audit of security policy, practice and procedure of ASIO, ASIS and DSD. Such an audit should be undertaken by the Australian National Audit Office, and should be conducted at relatively regular intervals.

1.22 The main reference points for the Committee's review were the revised PSM and the IGIS Inquiry recommendations, and to a lesser extent, a number of audits conducted by the Australian National Audit Office on protective security arrangements within selected Commonwealth agencies over the past three years.

1.23 The review focussed on the main components of the protective security framework adopted by each of the agencies, namely the security controls and procedures applied to personnel, physical and IT security, and the specific measures identified by the IGIS Inquiry to help strengthen security arrangements. To this extent, the findings of the IGIS Inquiry were considered central to the Committee's review.

1.24 Accordingly, the Committee wrote to the Prime Minister on 22 August 2002 requesting permission to include the IGIS Inquiry report as a formal exhibit to the review. In response, the Prime Minister stated in a letter on 24 November 2002, that the IGIS Inquiry report contained highly sensitive information and, as a result, would not be provided as a document to the Committee on security grounds. The Prime Minister did agree to allow Committee Members (and appropriately security-cleared staff of the Secretariat) to view the IGIS Inquiry report at the office of the IGIS.

1.25 The Committee noted that its inability to adopt the IGIS Inquiry report as a formal exhibit placed limitations on the review. The Committee did receive details of the IGIS Inquiry recommendations from each of the three agencies (including information on action taken to implement the recommendations) in their submissions, which enabled it to make some meaningful assessment of how the agencies had responded to the IGIS findings. However, the lack of formal access to the IGIS Inquiry report raised questions about the Committee's ability to perform fully the functions assigned to it under the *Intelligence Services Act 2001*, and whether security concerns would inhibit the Committee's ability to address other aspects of agency administration in future.

Protective Security Framework

1.26 The first step of the Committee's review was to briefly consider the protective security framework in place in each of the agencies. The ANAO notes that "a robust protective security control framework…directly influences the success and effectiveness of any policies developed for that agency's security environment, as well as the controls implemented to support it"[1]. The Committee was particularly interested in whether the framework established by each of the agencies included:

- a comprehensive organisational security plan based on risk assessment processes;
- clearly assigned responsibilities and accountabilities for managing security; and
- formal processes for reviewing security policy, practices and procedures.

Security Planning

1.27 The PSM places considerable emphasis on the need for agencies to develop and implement a security plan to effectively address their security risks. The PSM states that such a plan should be based on a security policy that supports the agency's goals and resources, and a thorough risk analysis. It should also be updated or revised on a regular basis or when the risk environment changes significantly[2].

1.28 ASIO reported that its main planning document, Security Management Plan 2001-2004, provides a strategic overview for the management of security within the organisation. It sets out the objectives and strategies relevant to managing security and addresses aspects of security to which all staff must adhere and which must be incorporated in the workplace. ASIO noted that it completed a security risk review and audit for all Australian offices in 2002 as part of a cyclical review and audit regime.

1.29 ASIS informed the Committee that it has an agency security plan, which addresses the range of risk management practices, security instructions and guidelines that ASIS apply to the conduct of business in Australia and

[1] ANAO, Protective Security Audit No. 23, 2002-2003, p.25

[2] Attorney-General's Department, Part B paragraph 4.9

overseas. This plan was based on a comprehensive risk review process, undertaken in the past two years.

1.30 DSD confirmed that it has a Security Plan which addressed the allocation of security responsibilities and resources, personnel security policies, and physical and IT security measures. DSD noted that its plan was linked to a comprehensive security risk assessment process, and had been reviewed to include recommendations from the IGIS Inquiry.

1.31 The Committee noted that security planning in each agency was clearly linked to security risk assessment processes, and effectively integrated into wider corporate management frameworks. It noted further that each agency had conducted comprehensive reviews of their security plans in the past three years to take into account recommendations of the IGIS Inquiry and significant changes to their security risk environment.

Assigned Responsibilities

1.32 The PSM advises that each agency should assign responsibilities for protective security management, and establish structures to help develop and implement security plans. The PSM proposes that agencies establish a security executive position, which is responsible for ongoing development and oversight of security policy, as well as designated positions for day-to-day management of security and information technology security specifically.

1.33 In evidence to the Committee, each of the agencies outlined how security responsibilities were assigned within their organisation, and the structures in place to administer those responsibilities.

1.34 ASIO currently has two corporate governance structures responsible for oversight of protective security. The first, the ASIO Security Committee (ASC), was established in 1996 following the Cook Security Inquiry, and includes representatives from senior management and all functional areas. The ASC's responsibilities include overview of: implementation and monitoring of integrated security policies; implementation and review of the agency security plan; the agency's Protective Security Risk Review (PSRR) process; and security audit functions. A second structure, the Security Coordination Committee, was established in 2001 to oversee implementation of the recommendations of the IGIS Inquiry. ASIO reported that this committee would be disbanded once implementation had been completed.

1.35 Within ASIS, security management responsibility is exercised by the ASIS Security Committee, which is chaired by the Director-General, senior executives from each of the agency's functional areas, and the Agency Security Adviser (ASA). This security committee is responsible for planning, management and oversight of the agency's security environment.

1.36 DSD noted further that it had established a senior security committee, comprising one-star officers, to develop and oversee the implementation of security policy and planning for the Directorate. This committee reports directly to the senior management group (which includes the Director General). DSD also has a designated Agency Security Adviser at the Senior-Executive Service (SES) level, and an IT Security Adviser position within its IT Section. Both these positions report to the senior management group on security issues.

1.37 The Committee notes that each of the agencies had established a direct line of communication and accountability between senior management and staff responsible for day-to-day management of protective security. Equally importantly, each agency had established structures to specifically address implementation of the IGIS Inquiry recommendations.

Security Audit Processes

1.38 Another essential part of the agency's security control framework are processes for monitoring and reviewing security practice and procedure. These processes enable agencies to assess how the security controls they've developed to treat security risks actually work.

1.39 The PSM advises that agencies should conduct regular security audits to ensure that protective security measures are being implemented efficiently and effectively. The IGIS Inquiry recommended that AIC agencies conduct comprehensive audits of their protective security arrangements at not more than 5-yearly intervals.

1.40 ASIO reported that it completed a risk review and security audit of all its domestic offices in 2002, as part of a cyclical audit regime. This process included reviews of security management plans for each site, physical and information security arrangements, and security clearance programs for staff. ASIO noted that the next risk review and security audit would be conducted in 2004-2005.

1.41 ASIS commenced a full audit of security in March 2003, in line with the recommendations of the IGIS Inquiry. ASIS said that its audit process consisted of twenty one work projects or packages addressing specific elements of protective security, which had been developed in consultation with the IASF.

1.42 The Committee received little information from DSD on its security audit mechanisms. DSD reported that it had a process in place to audit its security arrangements at regular intervals, and that this was monitored by the IASF's working group on physical and administrative security.

1.43 The Committee notes that each of the agencies also participates in the Protective Security Policy Committee (PSPC) annual security survey, which was developed to monitor agency compliance with PSM standards and guidelines.

Inter-Agency Security Coordination

1.44 One of the main themes of the IGIS Inquiry was the need for improved coordination and cooperation between AIC agencies in the management of protective security issues. The IGIS Inquiry recommended that the AIC agencies establish a formal inter-agency forum of senior staff with security responsibilities to address security issues of common interest, facilitate cooperation in the development and maintenance of security best practice within the AIC, and provide information and advice on security matters to agency management and the Secretaries' Committee on National Security (SCNS).

1.45 In response, AIC agencies and other relevant policy departments agreed to establish and participate in the Inter-Agency Security Forum (IASF), which commenced activities in 2001. The IASF currently manages three multi-agency expert working groups addressing personnel security, information management and physical and administrative security. The IASF and its three working groups have also assumed an important role in overseeing implementation by respective agencies of the recommendations of the IGIS Inquiry.

1.46 ASIO reported that the IASF has been active, at the working group level, in a number of areas. IASF has provided advice to agencies on the introduction of comprehensive security audit programs, and the development of minimum standards for conducting security clearance procedures at the Top Secret level. The IASF working groups were also developing advice on improving consistency in security policy and procedures in areas such as foreign contact and travel reporting, security incident reporting and the handling of accountable documents.

1.47 ASIO stated that the IASF's current focus was on facilitating greater consistency in the management of personnel security, enhancing security and audit features for office equipment and IT systems, and improving security standards for handling accountable documents.

1.48 The Committee strongly supports the work being undertaken by the IASF and its subsidiary working groups to establish security best practice guidelines and advice on new and enhanced security policies and procedures for member agencies. The Committee considers that the IASF's work should have particular benefit for the smaller agencies, and should contribute to raising protective security standards across all agencies.

1.49 The Committee questions whether there may be scope for the IASF to share information on its work with other Commonwealth and State agencies (such as state police) with comparable protective security needs. This could be particularly useful in areas such as information management and computer and telecommunications security.