2

Personnel Security

2.1 The first term of the Committee's review addressed the personnel security arrangements in ASIO, ASIS and DSD, including progress by the agencies in implementing the recommendations of the IGIS Inquiry. These arrangements include the management of security clearance programs, ongoing monitoring of staff security performance, and the conduct of security awareness training.

2.2 As agencies dealing almost exclusively with highly classified information, ASIO, ASIS and DSD are required to ensure that physical access to official information and resources is strictly controlled, and that those people who are granted access are reliable and fully understand their security responsibilities. This involves applying information security practices and procedures, based on the "need to know" (NTK) principle, applying and maintaining security clearances for all staff, and processes to support staff security awareness, including education and training.

2.3 In evidence to the review, each of the agencies emphasised that effective personnel security policy and practice was not only an integral part of their protective security control framework, but underpinned the overall security of their organisations. As one of the agencies stated:

> While we may have in place physical security measures and state of the art information security, it is the integrity of our staff that is the key to effective security. Physical and information technology security mechanisms afford little

> protection for capability and information if a determined insider can overcome them, if only for a short time.[1]

2.4 Accordingly, each of the agencies demonstrated a strong commitment to the development of a personnel security culture based on sound policies, practices and procedures.

2.5 The Committee found also that the agencies have made significant progress in implementing the recommendations of the IGIS inquiry on personnel security. This had resulted in changes to security vetting processes, particularly with respect to the re-evaluation and revalidation of security clearances, the introduction of security-related performance criteria, and new mechanisms for monitoring and auditing security practice.

2.6 The Committee identified a number of areas which may benefit from further attention. These include: the availability of administrative resources to conduct and re-evaluate staff security clearances; agency capacity to access information regarding employees that may indicate a potential security risk; and agency capacity to monitor and meaningfully analyse information on staff security compliance.

Security Clearances

2.7 Under the PSM, Commonwealth employees and contractors working with security classified information or in a secure area are required to hold a security clearance. For agencies processing and handling the most highly classified information, such as ASIO, ASIS and DSD, all employees are required to hold and maintain a security clearance at the TOP SECRET level.

2.8 Each of the agencies administers its own personnel security clearance programs, in accordance with the requirements and minimum standards outlined in Part D of the PSM. It is important to note that the Commonwealth expects that agencies working with highly classified material will maintain security clearance processes that exceed the requirements set out in the PSM.

2.9 Security clearances for ASIO personnel are conducted by the ASIO Counter-Intelligence and Security (CIS) Branch. The CIS Branch

[1] Private Submission, p.4

provides security support to staff on an ongoing basis, and assistance to other AIC agencies and Commonwealth entities in conducting staff security assessments. Security clearance processes for ASIS personnel are administered internally by ASIS Security Section.

2.10 Responsibility for administering security clearances for DSD personnel lies with the Defence Intelligence Group-Positive Vetting (DIG-PV) cell within the Department of Defence. DIG-PV also receives some assistance from ASIO in conducting staff security assessments.

Initial Vetting

2.11 All employees of ASIO, ASIS and DSD are subject to initial vetting, at the recruitment stage, and re-evaluation at later stages, to establish their suitability to hold and maintain a security clearance. As all employees are also required to hold security clearances at the TOP SECRET level, each agency is required by the PSM to conduct top secret positive vetting (TSPV).

2.12 The TSPV process involves an extensive and intrusive inquiry into an individual's life to establish their suitability to hold a clearance positively, beyond reasonable doubt. The evaluation of suitability is based on an examination of personal history, behaviour and character, and includes consideration of an individual's maturity, responsibility, tolerance, honesty and loyalty.

2.13 The TSPV process is very resource intensive and only conducted by certain specialist agencies, when the Government determines it is necessary. It includes:

- a review of documentation;
- comprehensive background checks;
- a personal interview; and
- referee contact

2.14 The TSPV processes of ASIO, ASIS and DSD include all of these components. However, they do differ in a number of ways; for example, in terms of the content and format of the personal interviews they employ, the number and mix of referees and the extent of background checking. As a result of the IGIS Inquiry, each of the agencies now also includes mandatory psychological assessment as part of its initial vetting and subsequent clearance review procedures (see below).

2.15 The agencies did not provide statistics on the time taken to process TSPV clearances at the initial stage, but indicated that the typical clearance period was 6-10 weeks once a case had been allocated to a case officer. At present there is a three month delay between the receipt of the completed forms and a case officer becoming available. Therefore the average time taken to process a TSPV is five months. While this is an improvement on the eight to twelve months it took a year ago, it is still above the target of three months for the entire process. After the Wispelaere and Lapas cases, Defence was issued with two not entirely compatible objectives: to increase the rigour of the process and to reduce the time taken. The first objective has been met and progress is being made on the second.

2.16 On the question of reliability, the agencies stated that they were confident that the TSPV programs that they had in place provided a sound basis for evaluating the suitability of staff to hold security clearances within their organisations. The agencies reported that the majority of TSPV clearance processes returned positive findings (reflecting the effectiveness of pre-employment screening), and no cases where security clearances were required to be withdrawn following re-evaluation.

2.17 The Committee recognises that, while uniformity remains an important principle and objective of Commonwealth vetting processes, the highly specialised and sensitive nature of the work undertaken by each of the agencies necessitates the ongoing development and application of organisation-specific assessment and evaluation procedures. This need limits the portability of security clearances at the TOP SECRET level. It also limits the extent to which agencies can contract out vetting components to external or private service-providers.

Psychological Assessment

2.18 The IGIS Inquiry recommended that agencies include psychological assessment as a mandatory pre-requisite for all TSPV clearances, and for subsequent clearance re-evaluations. It also recommended the establishment of an inter-agency body within the AIC to develop standards for psychological component of initial vetting and re-evaluation procedures.

2.19 ASIO, ASIS and DSD confirmed that they have incorporated psychological assessment procedures, involving psychometric testing and clinical evaluation, into their TSPV programs. ASIO and ASIS maintain a staff of in-house psychologists to conduct assessments, while DSD uses contract psychologists to perform initial recruitment assessment and utilises clinical staff employed by the Defence Security Branch (DSB) as part of the positive vetting.

2.20 Psychological testing methods and material vary between the three agencies, reflecting the differing organisational needs and suitability requirements of each. In response to the IGIS inquiry, agencies are working to develop a common model for psychological assessment procedures, and through the AIC Psychological Forum, draft minimum standards for use by all AIC agencies in psychological testing and evaluation.

2.21 The Committee supports efforts to develop AIC-wide standards for psychological assessment procedures. The application of these standards should enhance the consistency of testing, and the evaluation that such testing produces. This, in turn, should enable the exchange of more useful information on psychological assessment findings for job applicants and employment transfers within the AIC, and possibly remove some of the duplication in psychological assessment procedures that currently exists.

Additional Vetting Tools – Polygraph Testing

2.22 The IGIS Inquiry also recommended that agencies examine other tools that might enhance the reliability of their security clearance programs. In particular, it recommended that an AIC agency undertake a pilot study of the use of polygraphy for vetting, and that consideration also be given to the use of scientific content analysis (SCAN).

2.23 In its evidence to the review, ASIO confirmed that it had undertaken and completed a limited polygraph trial, involving ASIO volunteers, on behalf of AIC agencies in the second half of 2002. ASIO said the trial had been conducted on the basis of a strict ethical framework which had been developed in consultation with IGIS and other AIC agencies. The framework set parameters in regard to participation, the scope of examination questions, the use and protection of data and the handling of records.

2.24 ASIO did not provide details to the Committee on the results of the trial, but noted that it will prepare a report on the trial findings, in consultation with other AIC agencies and the Attorney-General's Department, which was referred to the Secretaries Committee on National Security (SCNS) for further consideration in December 2002.

2.25 The Committee accepts the need to develop new measures to continue to improve the reliability and accuracy of vetting processes. It notes that polygraph testing has been employed by a number of national security agencies in the United States for vetting purposes, and is considered a useful complementary screening instrument.

2.26 However, in the absence of details on the findings of the ASIO polygraph trial or information on the potential costs of administering a polygraph procedure, it is difficult for the Committee to comment on whether such testing is warranted or cost-effective at this time. The Committee urges each of the agencies to consider carefully the benefits and costs of adopting a polygraph procedure within their security risk assessment framework and wider corporate planning process.

Inter-agency Cooperation on Vetting

2.27 The IGIS Inquiry highlighted the need to strengthen further cooperation between the AIC agencies on recruitment and security clearance processes, particularly with respect to the sharing of security-related information on employment applicants and personnel holding TSPV clearances. The IGIS Inquiry recommended that the AIC agencies establish mechanisms to collect and exchange information on employment applicants that have been unsuccessful on security grounds, and on current employees seeking employment in other AIC agencies.

2.28 All three agencies confirmed that their recruitment procedures now require employment applicants to declare the results of previous applications for employment with AIC agencies and their consent to the disclosure of that information to other inquiring agencies, and the routine checking of applicant's employment history with other AIC agencies. To improve the efficiency of these procedures, the agencies agreed to the establishment of a common database of security-related information on applicants for all TSPV-level positions, and which would be accessible to all agencies.

2.29 ASIO reported to the Committee that the IASF's Physical and Administrative Security Working Group (PASWG) was developing proposals for a central register of information on people currently holding a TSPV clearance which would be maintained by ASIO, and which would be readily accessible to all agencies for employment purposes.

2.30 ASIS and DSD noted that they currently provide basic identifying details on all personnel holding TSPV clearances to ASIO, and also share security-related information on job applicants where requested by other agencies.

2.31 The Committee was satisfied that the measures recommended by the IGIS Inquiry, and currently being implemented by the agencies, will improve their ability to identify and assess employment applicants who have been rejected from other AIC agencies on security grounds or who may pose a security concern to their current employer.

2.32 The Committee emphasises that information-sharing between agencies on candidates for employment should be strictly limited to cases where applicants have been rejected on security grounds, and that access to such information should be governed by protocols agreed to by all AIC agencies.

Review of Security Clearances (Revalidation and Re-evaluation)

2.33 Under the PSM, Commonwealth agencies are required to re-evaluate the suitability of individual's to hold a security clearance on a periodic basis[3]. Such review mechanisms enable agencies to identify and assess changes that may have occurred in an individual's work and personal life, such as career development, significant relationships or change in financial status, and which may impact on the individual's suitability to hold a clearance. Periodic review of clearances also provides an opportunity, at least in theory, for agencies to determine whether a particular position, or function, requires a clearance at a particular level, or at all.

2.34 The PSM advises that for Designated Security Assessment Positions (DSAP's), agencies should, as a minimum, conduct a minor review

[3] Attorney-General's Department, op.cit. Part D, paragraph 8.1

of security clearances at 30 months (called re-validation) and a major review every five years (called re-evaluation).

2.35 Revalidation generally involves a security-related performance assessment and questionnaire completed by staff member and line manager, and a review of the staff member's personnel security file (PSF). The five-yearly re-evaluation process is more comprehensive, and as a result of the IGIS Inquiry, now essentially replicates the initial vetting procedure (including psychological assessment).

2.36 ASIO, ASIS and DSD emphasised that their security clearance review processes exceeded the minimum standards established by the PSM, and substantially met all the recommendations of the IGIS Inquiry. The agencies noted that in addition to standard revalidation procedures, they also conduct a special revalidation for all new staff after 5 months, which feeds into the probation report for new staff. The agencies reported that they also conducted ad hoc or "for cause" reviews of security clearances where circumstances required.

Managing Clearance Review Caseloads

2.37 The Committee was particularly interested in the management of clearance revalidation and re-evaluations workloads, given recent increases in employment numbers and the adoption of more rigorous procedures for re-evaluation as a result of the IGIS Inquiry.

2.38 All three agencies acknowledged that changes to re-evaluation procedures had placed more pressure on administrative resources, and the agency's ability to process re-evaluations within the PSM-required time limits. ASIO and ASIS noted that the recent expansion in recruitment, and resulting increase in the demand for initial vetting, had also had an impact on the resources available to process clearance re-evaluations.

2.39 Despite these pressures, ASIO reported that they had no prior or present backlog in the processing of revalidation and re-evaluation cases, and that all security clearance reviews were being conducted within acceptable timeframes.

2.40 DSD reported that there was a considerable backlog in re-evaluations. The average period before re-evaluation is approximately seven years rather than the five years required by the PSM. DSD is seeking to address this problem according to the following priorities:

- Reduction of the backlog on initial clearances;
- Re-evaluation for officers whose personal circumstances have changed, or whose annual re-evaluation may have suggested that issues may have arisen; and then
- Reduction in the backlog for everyone else.

2.41 ASIS reported in its submission that a percentage of its staff (including contractors) had not had their TSPV clearance re-evaluated in five or more years, and that a substantial portion of these were outside the 6 year mark. ASIS stated that all overdue re-evaluation cases had been surveyed and would be addressed in priority order with a view to completing the backlog by 2005.

2.42 The Committee accepts that TSPV security clearance and review processes will take longer than clearance procedures for lower security-classified positions. It also accepts that recent recruitment expansion in ASIO and ASIS has placed greater demand on vetting resources, and necessitated, in some cases, the prioritisation of security clearance-related work.

2.43 In this context, the Committee agreed that agencies should allocate vetting resources, as a first priority, to enable new positions supporting operational activities, to be filled as quickly as possible. However, the Committee also encourages agencies, and the IASF, to examine ways in which vetting resources can be shared, for example, psychological assessment services, to enable agencies to address short term delays in completing initial vetting or backlogs in TSPV re-evaluation processes.

Recommendation 1

That, as a first priority, the agencies address any existing or anticipated backlog in initial vetting and re-evaluation of TSPV security clearances to ensure that these processes meet PSM standards by 2003-2004 at the latest. Further, that the agencies include statistics on the number of outstanding TSPV re-evaluation cases and the times taken to process clearances in the reports made to this Committee as part of the annual review of administration and expenditure.

Personnel Security Monitoring

2.44 The PSM encourages Commonwealth agencies to consider measures to support their personnel security clearance processes, such as the provision of routine security briefings for staff and mechanisms to monitor and facilitate security performance.

2.45 Each of the agencies currently maintains a range of monitoring practices and activities designed to support its security clearance processes, and enhance security culture within the organisation more generally. These include annual security appraisals, use of security performance management, staff reporting requirements and staff survey processes.

Security Appraisals

2.46 In addition to the review procedures built into security clearance programs, each of the agencies also conducts routine appraisals of staff security conduct and awareness. To help reinforce sound personnel security practice, the IGIS recommended that agencies incorporate security-related criteria into their staff performance appraisal schemes.

2.47 In response, ASIO, ASIS and DSD have each taken steps to incorporate security appraisals into their overall staff performance assessment mechanisms. The security appraisal process developed by each agency focuses on staff attitude and conduct with regard to agency security policy, practice and procedures, and includes an evaluation of staff performance against identified security objectives. For example, DSD reported that its standard work performance agreement, negotiated between staff member and supervisor, includes a key measure of staff security attitude as part of each member's annual evaluation.

2.48 The Committee noted that agency procedures for monitoring staff security performance were well integrated into staff work performance appraisal schemes and broader security clearance review programs.

Security Reporting

2.49 As part of an effective risk management approach to personnel security, the agencies have in place a number of mechanisms to monitor staff activity, both in and outside the workplace, which may provide information about potential security risks.

2.50 Most immediately, the agencies utilise self-reporting and checking provisions included in the security clearance review process to get a picture of an individual's life situation, and a sense of their security health and probity. Staff are also required to report significant changes in their financial and personal circumstances in annual security appraisals and on an ad-hoc basis.

Staff Reporting Mechanisms

2.51 The IGIS Inquiry recommended that AIC agencies establish arrangements, where processes were not already in place, for reporting of and response to information concerning possible personnel security risks. It further recommended that agencies take steps to ensure that staff were adequately informed of and encouraged to use these reporting arrangements.

2.52 ASIO reported that it had formal procedures for staff to report information relating to possible security risks. It said that its CIS Branch maintained a list of information requirements which staff were asked to report on. These information requirements were updated regularly and re-issued to all staff. They included: identification of efforts to penetrate the organisation or compromise its functions; leaks of ASIO information; and other incidents involving ASIO staff, their families or colleagues that had counter-intelligence implications. CIS Branch was responsible for following-up this information, including the conduct of any resulting investigations.

2.53 ASIS confirmed that it had established a mechanism for reporting and responding to information concerning possible security risks, and that staff received appropriate training on how to identify risks. DSD said that it also had procedures in place for staff to report possible security concerns, and that information on how to follow these procedures had been communicated to all staff.

2.54 The Committee emphasises that staff reporting mechanisms are one of the most effective means agencies have to detect potential security risks, particularly where those risks involve the deliberate misuse by staff of official information and other official resources. It notes that reporting procedures in each of the agencies include clearly defined management and supervisory responsibilities for receiving and actioning information. This provides a level of institutional protection for staff, and discourages perceptions of an "informant" culture.

Financial Transactions

2.55 In addition to staff reporting processes, the agencies also have limited provisions, under Commonwealth legislation, to monitor information on financial transactions and taxation matters concerning staff which may indicate a potential security risk. These provisions allow the agencies , through ASIO, to access information held by AUSTRAC and the Australian Taxation Office. Such access is governed by memoranda of understanding (MOU's) between ASIO and the two bodies, and is subject to periodic oversight by the IGIS and this Committee.

2.56 In evidence to the Committee, ASIO emphasised that the primary function of the financial tracking facility was to assist agency operations, not surveillance of agency personnel. However, it noted that ready access to information on financial transactions allowed agencies to identify quickly one of the more obvious indicators of espionage activity – significant changes in the cash or asset holdings of staff.

2.57 The Committee considers that steps taken by the Commonwealth to enhance the agency's ability to identify and act on staff information that may signal a security risk are necessary and appropriate. In particular, it supports arrangements that enable AIC agencies, through ASIO, to access AUSTRAC's financial transaction reporting (FTR) database to check suspect transactions by personnel with TSPV clearances, and to access relevant information held by the ATO. This access is subject to strict controls, and periodic review.

2.58 The Committee further supports the recommendation of the IGIS Inquiry that the Commonwealth address the capacity of AIC agencies to obtain other relevant financial information on staff from sources such as credit reference agencies, and encourages the Commonwealth to look at improving agency access to information held by other financial institutions.

Recommendation 2

That the IASF review urgently areas where agencies are experiencing difficulties obtaining security-related information about personnel, such as the refusal by credit reference agencies to provide information direct to the Commonwealth, and develop proposals for appropriate legislative or policy action by the Commonwealth Attorney-General

Foreign Travel and Contact

2.59 Under the PSM, agencies are expected to establish arrangements to enable employees, both within and outside Australia, to report any contact with foreign government officials or people who have direct links to a foreign government agency, in line with the Commonwealth's Contact Reporting Regime[4].

2.60 This expectation was reinforced by the IGIS Inquiry, which specifically identified the need for AIC agencies to establish formal reporting regimes to monitor of staff travel overseas and contact with foreign nationals.

2.61 ASIO noted that the detailed contact reporting regime managed by ASIO's CIS Branch, includes reporting requirements on unauthorised contacts with individuals who may pose a threat to ASIO security. ASIO said it also managed a register of staff travel that was monitored by the CIS Branch. Information on travel and contact reporting requirements had been included in security awareness training packages and a revised security handbook for staff.

2.62 ASIS emphasised that it had established stringent procedures for reporting and action on foreign contact and travel prior to the IGIS Inquiry. All contact and travel information is processed centrally through the ASIS Security Section. ASIS noted that information on foreign contact and travel reporting requirements was included in its staff security handbook and periodically in administrative bulletins.

2.63 DSD advised that it had included information on staff responsibility to report contact with foreign national and non-official foreign travel to DSD's Security Section in its security awareness courses. It also published guidelines on definitions of foreign contact on DSD's intranet system.

2.64 On the basis of evidence presented to the review, the Committee concluded that the reporting regimes in place in each of the agencies were adequate. The Committee noted that the agencies had procedures in place to ensure that employees and supervisors were aware of their respective responsibilities in this regard, and designated resources to monitor and, where necessary, follow-up reporting information.

[4] Attorney-General's Department, op. cit. Part G

Security Awareness and Training

2.65 The PSM requires agencies to ensure that staff are aware of the threats the security controls in their work area are designed to counter, and their roles and responsibilities within the organisation's protective security framework. It does not advise agencies on how to facilitate staff security awareness, but does stipulate that some form of formal security training should be provided to all staff cleared to the SECRET or above level at least every five years as a condition of renewal of security clearance[5]

2.66 In evidence to the Committee, the three agencies emphasised that security education and awareness are critical facets of their personnel security programs, and are addressed continuously through specific training, security clearance review processes, routine appraisals and staff and administrative bulletins.

2.67 ASIO reported that all new staff attend either a two-day organisational orientation program, which has a security awareness focus, or the Generalist Intelligence Officers Training (GIOT) on commencement of duty. ASIO also require all staff and long term contractors to attend security awareness training at least once every five years, in compliance with the revised provisions of the PSM. ASIO noted that over 95 per cent of staff attended a formal security awareness briefing in the past five years[6].

2.68 ASIS emphasised that security awareness training was conducted continuously within the organisation, and promoted in all aspects of security and operational work. In addition to security briefing and training provided as part of introductory training for new recruits, ASIS also included security awareness components in its tertiary and operational training programs.

2.69 DSD stated that security awareness comprised a substantial part of the directorate's compulsory training program. All new staff are required to complete DSD's induction course, which includes a comprehensive session on security. After initial security training, DSD staff are also required to complete a security refresher course every two years. DSD noted that its staff courses including training for supervisors on skills to identify staff behaviour that may indicate possible security risk.

[5] Attorney General's, op.cit Section D, paragraph 8.48

[6] ASIO submission, p.15

Security Arrangements for Departing and Former Staff

2.70 The PSM provides limited advice on the security procedures for transferring and downgrading staff security clearances, but does not address security aftercare for personnel resigning or retiring from service. For high-level security agencies such as ASIO, ASIS and DSD, effective human management of former employees is important in ensuring that official information and assets continue to receive full protection.

2.71 The IGIS Inquiry highlighted this point, and recommended a number of measures to strengthen the aftercare programmes of high-level security agencies with respect to departing and former staff. These included: inclusion of security-based interviews and psychological assessment of staff prior to separation; agency review of cases where exit interview and psychological assessment do not take place; and use of ex-staff associations as a source of information on the welfare and other concerns of former employees.

2.72 ASIO reported that all staff participated in an exit interview as part of the separation process. This interview was designed to address relevant security issues and remind staff of their security responsibilities post-employment. ASIO confirmed that it also conducted psychological assessments, and provided counselling, for departing staff. ASIO noted that it also provides some administrative support for an ex-officer’s association.

2.73 ASIS informed the Committee that its staff exit procedures already included most of the measures recommended in the IGIS Inquiry, and that consideration was being given to the further requirement that former staff inform ASIS of any post-employment activity of a security nature. ASIS stated that it did not have an ex-staff association at present and did not intend to establish one in the foreseeable future. ASIS had in the past attempted to set-up and foster a body for former staff, but these had foundered.

2.74 DSD confirmed that its staff exit procedures required staff to participate in a security-based debriefing session, which included information on ongoing security responsibilities, and an exit interview with a trained psychologist or human resources staff member to address any issues that may lead to future security problems. DSD does not maintain an ex-staff association. However, former DSD employees have access to a range of formal and informal support mechanisms provided by the Department of Defence.

2.75 The Committee considers that, on the basis of information provided to the review, agency security arrangements for departing and former employees are adequate. They address the need to ensure that departing staff are fully informed about their ongoing responsibilities to protect information, and have the opportunity to discuss issues of concern prior to departure. They also provide a level of professional and personal support for individuals in the transition out of a highly secure work environment (and all the information restrictions that that entails) and, to a more limited extent, ongoing aftercare for former employees.