10

Audit Report No. 23, 2002–2003

Physical Security Arrangements in Commonwealth Agencies

Introduction

Background

10.1 Protective security encompasses information, personnel, physical, information technology and telecommunications security. The Commonwealth's Protective Security Policy is outlined in the Protective Security Manual (PSM) which provides specific guidance to agencies on the protection of the Commonwealth from potential security threats.[1]

10.2 Part E of the PSM outlines the Commonwealth's physical security policy, including the recommended physical security framework, procedures and minimum standards.

[1] Auditor-General, *Audit Report No. 23, 2002–2003, Physical Security Arrangements in Commonwealth Agencies*, Canberra, December 2002, p. 13.

10.3 In recent years, changed work practices such as an increasing reliance on information technology, contracting and home-based work practices have exposed the Commonwealth to new vulnerabilities and risks. In addition the international and domestic security environment has been changed by the impact of events such as the terrorist attacks in September 2001 and the Bali bombings in October 2002. These events have created a heightened awareness of the range of risks to be managed by Commonwealth agencies.

10.4 To maintain a secure environment, such risks and vulnerabilities need to be understood, prioritised and managed to prevent the occurrence of harm (defined in the PSM as any negative consequence), such as compromise of or damage to or loss incurred by the Commonwealth.

The audit

10.5 The audit evaluated the security policies and practices of seven Commonwealth agencies to determine whether they had established an appropriate physical security control framework based on the principles outlined in the PSM.

10.6 Specifically the audit examined whether the agencies had:

- assigned roles and responsibilities for security;
- undertaken an appropriate Security Risk Assessment process prior to developing the Agency Security Plan;
- documented and implemented an effective set of controls and procedures to limit the impact and/or consequence of their identified security risks to an acceptable level;
- educated staff in their responsibilities and duties within the security environment; and
- considered the risk, and developed an appropriate policy statement on the physical security arrangements for employees who work from home.[2]

Audit findings

10.7 The audit report concluded that all the audited agencies had made reasonable progress towards meeting their physical security responsibilities as outlined by the PSM. In general this resulted in the

[2] Auditor-General, *Audit Report No. 23, 2002–2003,* p. 14.

establishment of a protective security control framework capable of limiting their exposure to physical security risks.

10.8 However, a number of deficiencies were identified which could have had a negative impact upon the integrity of the protective security environment. The report found that agencies were not:

- undertaking regular comprehensive protective security risk assessments;
- formally considering the physical safety of staff as part of the risk assessment process;
- establishing a clear link between the risk assessment process and procedure development;
- maintaining adequate and current documentation to support the security risk, cost benefit analysis and decision-making processes;
- consistently applying internal controls and procedures, thereby undermining their effectiveness;
- educating their staff, contractors and clients of agency security standards; and
- monitoring the effectiveness and cost-efficiency of the security environment and acting on identified deficiencies in a timely manner.[3]

10.9 The audit report noted that deficiencies in the physical security segment of a protective security framework needed to be considered in conjunction with other aspects of the protective security. This was because an exposure in one part of the framework could result in increased exposure on an agency-wide level.

10.10 The report also noted that the audit was undertaken at a time when Commonwealth agencies were operating in a heightened international threat environment, following terrorist attacks in New York and in Bali. These events added weight to the report's conclusion that agencies needed to move to a proactive protective security approach.

10.11 The report emphasised that Commonwealth agencies now operated in an environment where they were required to acknowledge that threats and risks once thought unlikely must now be considered as possibilities.

10.12 The report's findings were supported the Attorney-General's Department following work undertaken by the Protective Security Coordination

[3] Auditor-General, *Audit Report No. 23, 2002–2003,* p. 15.

Centre. The Centre had found that agencies had a weak and reactive approach to maintaining their protective security responsibilities.[4]

The Committee's review

10.13 On 21 May 2003, the Committee held a public hearing to review the progress made by the relevant agencies in relation to the implementation of the ANAO's recommendations.

10.14 The Committee took evidence from the following agencies:

- Department of Prime Minister and Cabinet (PM&C);
- AirServices Australia;
- Australian Nuclear Science and Technology Organisation (ANSTO); and
- Parliament House Security Board.

10.15 The Committee took evidence on the following issues:

- security education and awareness;
- security risk assessment; and
- incident management and reporting.

Security education and awareness

10.16 The audit report emphasised that security regimes were only effective if everyone involved in adhering to the requirements was aware of their responsibilities and consistently applied the identified controls. It also noted that agencies were required by the Commonwealth, as documented in the PSM, to ensure that the staff, contractors and clients were made aware of and were regularly briefed on the security requirements of the agency. [5]

10.17 The report stated that:

> Agencies should develop education and awareness programs based on the security standards and documented procedures of the agency. These should be communicated to staff when they commence with the agency, and then on a periodic (at least annual) basis thereafter as part of a security refresher awareness

[4] Auditor-General, *Audit Report No. 23, 2002–2003,* p. 17.

[5] Auditor-General, *Audit Report No. 23, 2002–2003,* p. 48.

> program … Agencies can also make use of information circulars to advise staff, in a timely manner, of new or revised standards.[6]

10.18 The audit found that not all of the agencies provided this level of staff training. Four of the agencies did not provide new starters with training and in five of the agencies involved in the audit, the on going training was found to be 'insufficient, of low quality and not provided to all staff'.[7]

10.19 The Committee questioned the agencies attending the hearing about provision of security training within their organisations.

10.20 All agencies present described processes involving security training in the induction package s of new starters and several indicated that, since the audit, they had begun the practice of refresher security training for all staff. PM&C stated:

> Last year we conducted a security awareness refresher course for all staff; that was conducted by the training officers from the Protective Security Coordination Centre. We are proposing that that will be an annual event.[8]

10.21 ANSTO noted that:

> We have also had recently … security awareness seminars for everybody on the site, which involved getting in some expert lecturers from outside the organisation to discuss the various aspects of security.[9]

10.22 AirServices Australia explained the devolution of security responsibility to business centres but outlined procedures that ensured security training was ongoing, even for employees of long standing:

> [Business centres] report to us. They provide routine reports … about the scope and the nature of the training that is conducted and the numbers of people attending. [If they were not including security training] we would remind them of what their obligations are for particular training.[10]

10.23 On behalf of the Parliament House Security Board, both the Department House of Representatives and Department of the Senate indicated that they were trialling online security training as an ongoing refresher training option.

[6] Auditor-General, *Audit Report No. 23, 2002–2003*, p. 48.

[7] Auditor-General, *Audit Report No. 23, 2002–2003*, p. 48.

[8] Mr Terry Crane, *Transcript*, 21 May 2003, p. 112.

[9] Mr Steven McIntosh, *Transcript*, 21 May 2003, p. 111.

[10] Mr Michael Howard, *Transcript*, 21 May 2003, p. 112.

10.24 However, Parliament House Security Board also indicated a number of challenges to providing staff with initial and refresher training in security awareness. While departmental staff were catered for by the separate parliamentary departments, Members of Parliament and their staff were not. A representative of the Board explained:

> We have quite an issue in communicating with the occupants of [Parliament House] because of their itinerant nature and that is something that we should be taking on board.[11]

10.25 PM&C also highlighted the difficulty in providing time for additional training, and the importance of creating a culture of responsibility among all staff, noting that:

> The level of training that we provide to our staff is probably the maximum we could provide under the circumstances. If I were looking to mandate two or three days of training for each member of staff, I would have great difficulty … Having said that I think we do provide a good balance. People in Prime Minister and Cabinet are well aware of their responsibilities and we do stress to them that I am not the person responsible for security in Prime Minister and Cabinet, each and every person that works in that department is responsible for the security.[12]

Incident reporting and management

10.26 The audit report noted that the integrity of the security environment was strengthened where agencies took a proactive approach to the monitoring, response and reporting of incidents that have resulted in a security breach.

10.27 The report emphasised that it was crucial for agencies to respond to incidents in a structured, thorough and timely manner. This included the timely recording and investigation of security incidents, analysis of the information gathered for the investigation and incorporation of the information into the agency security plan.

10.28 The audit report also noted that only two agencies were able to demonstrate that they enacted any form of discipline for security breaches committed by staff.[13]

10.29 At the public hearing the Committee sought clarification from agencies on how they responded to security breaches by staff.

[11] Mr David Elder, *Transcript*, 21 May 2003, p. 114.

[12] Mr Terry Crane, *Transcript*, 21 May 2003, p. 116.

[13] Auditor-General, *Audit Report No. 23, 2002–2003*, p. 84.

10.30 Agencies explained that they responded to staff security breaches with a range of options, depending upon criteria such as whether the incident was a 'one off' or a repeat offence and the severity of the breach. Agency disciplinary responses included the following:

- placement of letter on personnel file;[14]
- request for written explanation of breach;[15]
- reference to breaches during performance appraisal;[16]
- withdrawal of access;[17] and
- possible dismissal.[18]

10.31 The Committee raised the breach of ANSTO's perimeter by Greenpeace protesters on 17 December 2001. The Committee questioned ANSTO on how it had responded to the incident.

10.32 ANSTO pointed out that although the security guards attempted t o prevent the breach, they were limited in their powers:

> The APS Act limits [guards] from using force unless lives are in peril, basically. They made a judgement on the day that this was a political protest, lives were not in peril and, therefore they were not entitled under their act to use force. We have taken a number of physical security steps since, but we did not see that there was scope for disciplining anybody for that action, because they were prohibited by their Act from doing anymore than they did.[19]

10.33 The Committee noted reference in the audit report to the limitations of over-reliance on security guards and that during its fieldwork the ANAO had observed a number of breakdowns in the application of controls by security guards.[20]The Committee cited incidents of personal experiences where this had also happened.[21]

[14] Mr Michael Howard, *Transcript*, 21 May 2003, p. 108.

[15] Mr Terry Crane, *Transcript*, 21 May 2003, p. 109.

[16] Mr Terry Crane, *Transcript*, 21 May 2003, p. 109

[17] Mr Steven McIntosh, *Transcript*, 21 May 2003, p. 109.

[18] Mr Michael Howard, *Transcript*, 21 May 2003, p. 108

[19] Mr Steven McIntosh, *Transcript*, 21 May 2003, p. 109.

[20] *Transcript*, 21 May 2003, p. 107.

[21] *Transcript*, 21 May 2003, p. 109.

10.34 The audit report also noted that guards may be less effective if, as was observed, they were overloaded with operational and management duties as well as being expected to respond to security breaches.[22]

10.35 Agencies were asked to comment on these criticisms and responded by explaining the range of controls used to ensure the physical security environment. This included:

- guards placed at high risk points, particularly entry / exit points;
- surveillance systems, including recording systems and CCTV;
- electronic alert mechanisms;
- physical barriers; and
- reliance on intelligence from Australian Security Intelligence Organisation (ASIO), the Protective Security Coordination centre (PSCC) and the Australian Federal Police (AFP).[23]

Security risk assessment

10.36 The audit report recommended that all Commonwealth agencies be required to undertake an appropriate and thorough protective security risk assessment process at least every three years.[24]

10.37 However, the PSCC stated that agencies should review and update their security plans and risk assessments on an annual basis, particularly taking account of ad hoc security reviews that may have arisen from security breaches.[25]

10.38 The Committee noted that the audit report criticised agencies for not integrating their learning from ad hoc security assessments into their existing control frameworks.

10.39 At the hearing the agencies responded with explanations of risk assessment processes that generally contained similar actions and procedures. For example, PM & C stated:

> …we undertake regular internal reviews and also risk assessments, and we have certainly done so since the issuing of the general security alert by PSCC in November 2002. The recommendations of those reviews have been acted upon and we

[22] Auditor-General, *Audit Report No. 23, 2002–2003*, p. .

[23] *Transcript*, 21 May 2003, pp.107–108.

[24] Auditor-General, *Audit Report No. 23, 2002–2003*, p. 44.

[25] Auditor-General, *Audit Report No. 23, 2002–2003*, p. 42.

> have incorporated much of that into our security plan which was issued in September last year. Since then we have reviewed our internal arrangements on a number of occasions.[26]

10.40 Two of the agencies present indicated that they utilised the PSCC risk management training courses and materials for relevant staff. All indicated that they had formal risk assessment processes that took account of security risk assessment as part of the overall risk asses The Committee is pleased to note that the agencies have responded in a timely and appropriate manner to the recommendation that agencies develop and schedule periodic formal education and awareness programs for all personnel.[27]

Committee comment

10.41 The Committee acknowledges that all agencies have constraints that affect the manner in which they provide security training. Clearly, each agency must look for ways to address the security framework in the most effective and efficient way for the organisation involved. However, it is incumbent upon agencies to ensure that training is relevant, accessible to all staff and maintains staff knowledge to current security standards.

10.42 The Committee is pleased to note that agencies are aware of the importance of a thorough and timely response to security breaches and the importance of incorporating learnings gained from breaches into current security controls.

10.43 The Committee notes that the ANAO report contains suggestions and examples of better practice which may be of use to Commonwealth agencies in providing a secure physical environment. The Committee encourages agencies to examine the potential lessons in the report.

[26] Mr Terry Crane, *Transcript*, 21 May 2003, p. 111.

[27] *Transcript*, 21 May 2003, pp. 110–11.