4

Information Technology Security

4.1 The fourth term of the Committee's review addressed agency security arrangements with respect to information technology (IT) processes and systems, including the implementation of measures for computer security recommended by the IGIS Inquiry. For the purposes of the review, the Committee focused on the range of security measures applied by agencies to protect information processed, stored and transmitted by computing systems (referred to as COMPUSEC).

4.2 The Committee's starting point was the Commonwealth's Protective Security Manual 2000 (PSM), and the guidelines it provides on the protection of electronic-based information. As with other parts of the review, the Committee's objective was not to conduct an exhaustive audit of agency's IT security policy, practice and procedure with respect to the PSM, but to obtain an overview of IT security controls and processes, and work done by the agencies to address the findings of the IGIS inquiry in particular.

4.3 As evidence to the review made clear, IT security is assuming increasing importance to government agencies dealing with sensitive information. Greater reliance on electronic communication, and the shift from paper-based filing and information management systems, has meant that the role of IT security within these organisations has grown dramatically in the past ten years.

4.4 In this context, it is worth noting that the three agencies have always maintained a high degree of IT security to help secure their capability and intelligence from compromise. The IGIS Inquiry provided further impetus to agencies' efforts to improve the security of their computing and communication systems, and the way IT security fits into overall protective security frameworks.

4.5 In general terms, the Committee is satisfied that the agencies continue to assign high priority, and accord sufficient resources, to the maintenance and improvement of IT security. Evidence provided to the review suggests that the IT security controls, practices and procedures in place at each of the agencies adequately meet the standards set out in the PSM, and in many areas, exceed them.

4.6 The Committee notes that the work of the agencies in implementing the recommendations of the IGIS Inquiry on computer security is well advanced, and should be substantially completed within the next twelve months. Areas requiring further attention include: the use of biometric access controls for computer systems; the development of systems to ensure the application of "need-to-know" restrictions to all electronic information; and improving the capability of agencies to effectively audit information on access to and use of IT systems.

Responsibility for IT Security

4.7 The PSM expects that agencies, in developing their protective security frameworks, will assign responsibilities and allocate resources specifically for the management of electronic communications networks. It recommends that agencies establish an IT Security Adviser (ITSA) position, and that this position works closely with the Agency Security Adviser (ASA) to ensure that security measures taken to protect IT&T systems are integrated into the agency's total security control framework.

4.8 Each of the agencies demonstrated that they have taken necessary steps to assign responsibility for IT Security within senior management and to establish structures to develop, apply and maintain IT security policy.

4.9 ASIO maintains an IT Security Directorate which is separate from the organisation's IT branch and reports directly to the Manager of Counter-Intelligence and Security (CIS). ASIO reported that it had

increased the number of staff in the IT Security Directorate to fourt, including the appointment of a Director, in the past two years.

4.10 ASIS has an IT security unit, headed by an IT Security Adviser (ITSA), which oversees the integrity of ASIS data storage and transmission systems, and which reports directly to the agency's security section.

4.11 DSD maintains a designated IT security section, which is autonomous from IT administrative, support and project staff. The IT security section is answerable to the Directorate's Central Management Committee through a senior executive officer responsible for IT management.

IT Security Accreditation

4.12 The PSM expects that agencies will consider IT systems, and systems security in particular, in the context of its risk assessment process for information security, and adopt appropriate measures and procedures. Further, it expects that agencies will take steps to ensure that the measures it implements are independently assessed and accredited by the Commonwealth (either through DSD or an evaluation facility established under the Australian Information Security Evaluation Program).

4.13 In evidence to the Committee, each agency confirmed that its IT&T requirements had been subject to risk review and treated accordingly. They also confirmed that the security measures they applied to their computing systems were independently evaluated and accredited in line with the PSM.

Computer Security Measures

4.14 The PSM itself provides limited guidance to agencies on the security measures they are required to apply to IT systems to ensure that they provide adequate protection for security classified information. More detailed guidelines on Commonwealth requirements for communications and electronic security are provided by the Australian Communications and Electronics Security Instructions (ACSI) 33, issued by DSD's Information Security Group.

4.15 Together, the PSM and ACSI 33 require agencies to use logical access controls to restrict access to computer networks. It also requires agencies to establish IT system audit trails and other

procedures and controls to ensure that IT systems and networks are not compromised (for example, by viruses or damaged software).

4.16 The IGIS Inquiry directed agencies to include comprehensive and "upgradeable" security measures in the design of all computer systems carrying highly classified information. Such measures typically include user identification and authentication, screen locks and clearers, hard data encryption, audit trails and logs, and firewalls and other controls to restrict unauthorised access to networks. The Committee did not take detailed evidence on all IT security measures applied by the agencies, but did consider a number of areas highlighted by the IGIS Inquiry.

4.17 ASIO said that it had made significant changes to its internal computing systems to maintain best security practice, and that these changes would be ongoing. Both ASIS and DSD confirmed that they were in the process of upgrading their IT platforms to include comprehensive security measures, and that these measures would be "upgradeable" as systems technology changed.

Applying Need to Know Restrictions

4.18 The IGIS Inquiry further identified the need for AIC agencies to take steps to ensure that their computer systems can enforce need-to-know (NTK) restrictions placed on security classified information. It also recommended that agencies establish procedures to ensure that an individual's access to NTK material held on computer systems is reviewed as his or her duties or the nature of the information holdings change.

4.19 All three agencies stated that they had a range of controls to enforce NTK restrictions placed on information. ASIO said that it was confident that the security features of its IT systems enabled NTK restrictions to be effectively applied to its electronic-information. ASIO did not provide information on its arrangements for reviewing user access to security classified information holdings.

4.20 ASIS reported that, in addition to standard logical access controls, it also utilises Access Controls Lists (ACL) to restrict user access to security classified information. Changes to ACL's required authorisation from line managers and could only be effected by a limited number of authorised IT security staff.

4.21 DSD outlined a number of security features of its computing systems that support NTK restrictions. These included: individual

(certificate-based) authentication of users; user identification and password required for systems access; and systems access approval on a case-by-case basis. DSD noted further that it was working to develop controls to improve its ability to review access to NTK material quickly and easily. At present, user access is audited and provided to the owners of the data for review.

Access Controls

4.22 The PSM requires agencies to have the means to control access to their computer systems and networks, regardless of whether the system carries security classified information or not. This typically requires the application of logical access controls to computer systems based on user identification and authenticators (for example, passwords) for each user, including procedures for limiting access to information within those systems.

4.23 In addition to these controls, the IGIS Inquiry recommended that the agencies implement biometric access controls for computers carrying security-classified information.

4.24 ASIO did not provide any details on its IT access controls, but indicated that these were in conformity with the PSM and adequate given the level and extent of its security-classified information holdings. It noted that it was examining possible options for applying biometric access controls for computers linked to classified networks, including a biometric system currently being evaluated by the Australasian Information Security Evaluation Program.

4.25 ASIS reported that it utilises standard logical access controls in accordance with the PSM. These included user identification and password protection, as well as password protocols such as minimum password lengths, specific formatting and appropriate frequency of password change. ASIS noted that it had not commenced work on biometric access controls for its computing systems. ASIS said it would consider the findings of continuing IASF research into biometric technology before making a decision on implementation.

4.26 DSD confirmed that its computing systems and networks include logical access controls to restrict access to authorised users. It also confirmed that it was researching biometric access control technology to assess its suitability for DSD's IT environment, but did not expect work on implementation to begin this year.

4.27 The Committee strongly supports the introduction of biometric access controls to agency computing systems. This should further enhance the agency's ability to limit access to highly classified information to those individuals with an authorised need-to-know, and improve their capacity to track use of classified information held on secure system. It encourages the agencies to examine biometric options that can be adapted to their physical security framework as a physical access control at a later date.

Other IT Controls

4.28 The PSM and ACSI 33 identify a number of other IT security controls that agencies should maintain depending on the level of security classified information they hold. These include: encryption of electronic data ; identification and authentication for all software; restrictions on personal computer connections to local area networks (LANS), wireless area networks (WANS) and public networks such as the internet; use of firewalls to control and audit access between networks; and computer virus and other intrusion detection mechanisms.

4.29 The Committee notes that each of the agencies has strict policies and procedures to ensure that their computing and communications networks are not directly connected to 'untrusted' systems. Each also utilise firewalls to protect systems and data where networks are linked to those of other agencies. All three agencies also utilise encryption devices accredited by DSD for the electronic transmission of security classified information.

IT Audit Capability

4.30 The IGIS Inquiry highlighted the need for agencies to improve their capacity to generate and audit information about access to and use of their IT systems, and classified networks in particular. It recommended that agencies include advanced auditing features, as they become available, in their computing systems, and take steps in the mean time to ensure that their computing systems are capable of recording what information users access and what documents they print out.

4.31 ASIO reported that it has funded an "Audit Project" to research and implement a solution which meets the IGIS directive. The project was designed to establish an audit capability that meets a high

proportion of organisational requirements. ASIO said it expected that the audit solution would be fully implemented by mid-2003.

4.32 ASIS similarly confirmed that it had allocated resources to developing an advanced audit capability for its IT systems. ASIS said that it had set up a project to examine auditing and logging and the application of NTK restrictions, with a view to establishing an integrated system for data holdings and centralised auditing and logging functions.

4.33 DSD reported that it had reviewed and revised its IT auditing strategy, and is in the process of developing tools to provide advanced auditing features, alerts and pattern analysis where necessary. DSD had also implemented a number of measures for selected systems, including: auditing of data searched, data read and data printed; and the review of audit reports by data owners on a monthly basis.

4.34 The Committee was generally satisfied that the agencies have taken appropriate steps to identify, study and evaluate all options for expanding their IT audit capability. It notes that both ASIO and DSD set firm deadlines for implementation of additional audit measures, and encourages ASIS to establish a timeframe that is consistent with deadlines for other outstanding IGIS Inquiry recommendations.

IT Security Awareness

4.35 While staff IT security awareness and training was not addressed in any detail by the PSM or the IGIS Inquiry, the Committee was interested in agency activity in this area. Each of the agencies emphasised the important role staff security awareness played in supporting its IT security controls and procedures.

4.36 ASIO noted that a primary focus of the work of its IT Directorate was to provide IT security awareness training for both technical and non-technical staff across corporate and operational activities. ASIO reported that it had developed and implemented a course structure on IT security awareness, with a view to providing scheduled formal training for all staff every six months.

4.37 ASIS indicated that IT security education and training was an important part of its information security framework, and that all staff received training on IT security requirements at induction and periodically during their employment.

4.38 DSD noted that it applied a number of controls and procedures to reinforce staff awareness of IT security requirements. This included: briefing on IT security regulations, monitoring and auditing activity for all new staff; use of computer screen banners notifying staff of their security responsibilities and activities; and educational and other specialised training programs designed to maintain staff security awareness.