Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

INTRODUCTION

Version 1.0

Introduction

101. Commonwealth Government agencies are required by the Protective Security Manual (PSM) to consider the security implications of their electronic information systems and to devise policy and plans to ensure the systems are appropriately protected. Although security needs will be greatest when National Security classified or Non-National Security classified information is being processed, even unclassified systems with no special safety, mission critical, or financial implications should have some degree of protection if a reliable or accurate service is to be maintained. The Australian Communications-Electronic Security Instruction (ACSI) 33 has been developed by the Defence Signals Directorate (DSD) to provide guidance to Australian Government agencies wishing to protect their information systems.

102. ACSI 33 terminology is consistent with the PSM. In particular it adopts the following terms:

a. "National Security classified" - information classified **RESTRICTED**, **CONFIDENTIAL**, **SECRET**, or **TOP SECRET**.

b. "Non-National Security classified" - information classified **IN-CONFIDENCE**, **PROTECTED**, or **HIGHLY PROTECTED**.

c. "Classified" - information which is either National Security or Non-National Security classified.

d. "Unclassified" - all other information.

Scope and Audience

103. This publication discusses the security issues for all Commonwealth Government electronic information systems, whether they process classified information or other critical but unclassified information, and regardless of whether they are a large or small, multi-user or single-user system. Electronic information systems in this context include but are not limited to: computer mainframes, servers and workstations; their hardware, software, firmware, operating systems, packages, applications and data storage; communications devices with data storage facilities (eg message switches, packet switches, routers and bridges); systems that contain embedded processors; and PABX systems.

104. The ACSI 33 ***is not*** intended for those staff with little or no technical understanding of the relevant security issues, general agency staff or agency executives. Specifically, it is intended for the following staff:

a. Agency IT security administrators, system and network administrators;

b. Agency IT Security Advisers;

c. Agency Security Policy staff;

d. Technical personnel with some IT security responsibilities;

e. Security personnel with some IT security responsibilities and understanding; and

f. Outsourcing agencies and agents acting on their behalf.

ACSI 33 Structure

105. The ACSI 33 is essentially a series of publications, each one a 'handbook' covering a specific topic. Users should note that each handbook is subject to amendment, and as such has been afforded its own version number and version date.

106. Each handbook discusses the relevant security issues and, where appropriate, endeavours to categorise the security countermeasures into identified risk levels, defined as "grades". These grades have been formulated and included to facilitate the application of minimum standards and recommendations. All minimum standards are contained in **Handbook 1 - Standards**.

107. The ACSI 33 has been written to be consistent with the PSM, and with two Australian Standards, namely the AS/NZS 4444:1999 and AS/NZS 4360:1999. The AS/NZS 4444:1999 entitled "Information Security Management" defines a comprehensive list of IT security controls. These controls are not duplicated in the ACSI 33 handbooks, and users should obtain copies of this standard from **Standards Australia**. Although **Handbook 3** provides a worked risk management example, the AS/NZS 4360:1999 further defines the "Risk Management" standard, and can also be obtained from Standards Australia.

DSD Advice and Assistance

108. By Cabinet Directive, DSD is required to provide material, advice and assistance to Commonwealth Government agencies and the Australian Defence Force where there is a threat to national security in respect of "information that is processed, stored, or communicated by electronic or similar means". Similarly, DSD is charged with providing advice and assistance on request where the information is unrelated to national security but still requires protection from unauthorised disclosure or manipulation. Agencies are encouraged to contact DSD for advice and assistance, through their IT Security Adviser (ITSA) or Agency Security Adviser.

Contacts

109. The following are links to those organisations that have some role in security of Government systems:

DSD Information Security Group
General IT security advice, risk assessment, system security assessment and advice on system security products.

Attorney-General's Department
Protective Security Coordination Centre. General security training including IT security training.

Privacy Commissioner
Privacy standards and guidelines for IT systems.

ASIO T4 Protective Security Group (02) 6234-1207
Advice on physical security, risk assessment, evaluation of physical security products and physical security reviews.

Australian Security Vetting Service (Attorney-General's Department)
Vetting of personnel.

Commonwealth Law Enforcement Board
Fraud policy and prevention, and general law enforcement issues.

National Office for the Information Economy
IT security guidelines and PKI standards. The Gatekeeper site can be found at **http://www.gpka.gov.au/**.

National Archives of Australia
Advice and guidelines on Archives legislation and its application to computer systems.

References

110. The following unclassified publications contain guidelines relevant to the security of Commonwealth Government information systems.

Protective Security Manual
Source: Attorney-General's Department
Content: Guidelines on all aspects of security for the Commonwealth Government, including IT Security.

Evaluated Products List (EPL)
Source: DSD Advice and Assistance Group
Content: The EPL contains a list of products that have been certified by DSD under the Australasian Information Security Evaluation Programme (AISEP). This list, which includes encryption products approved by DSD, is updated quarterly, and is published in hardcopy and on the DSD website.

Gateway Certification Guide
Source: DSD Advice and Assistance Group.
Content: A guide for agencies seeking DSD certification of their public network gateway.

Best Practice for Fraud Control
Source: Attorney-General's Department. Commonwealth Law Enforcement Board.
Content: All aspects of fraud control, including guidelines on information exchange.

Keeping Electronic Records
Source: Australian Archives
Content: Policy for electronic record keeping in the Commonwealth Government.

Information Security Management (AS/NZS 4444:1999)
Source: **Standards Australia**
Content: Guidelines on information security.

Risk Management (AS/NZS 4360:1999)
Source: **Standards Australia**
Content: Guidelines on risk management.

An Introduction to Computer Security: The NIST Handbook
Source: National Institute of Standards and Technology
U.S. Department of Commerce
Content: Guidelines on IT security.