The Auditor-General

Audit Report No.13 2001–2002

Performance Audit

Internet Security within Commonwealth Government Agencies

Australian National Audit Office

© Commonwealth
of Australia 2001

ISSN 1036-7632

ISBN 0 642 44271 1

COPYRIGHT INFORMATION

Australian National
Audit Office

Canberra ACT
20 September 2001

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit across agencies in accordance with the authority contained in the *Auditor-General Act 1997.* I present this report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Internet Security within Commonwealth Government Agencies.*

Following its tabling in Parliament, the report will be placed on the Australian National Audit Office's Homepage—http://www.anao.gov.au.

Yours sincerely

Ian McPhee
Acting Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office. The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

Auditor-General reports are available from Government Info Shops. Recent titles are shown at the back of this report.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone (02) 6203 7505
Fax (02) 6203 7519
Email webmaster@anao.gov.au

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team

Dr Paul Nicoll
Michael McFarlane
Belinda Conn

Contents

Summary and Recommendations

Audit Findings and Conclusions

Appendices

Abbreviations

ABN–DSC	Australian Business Number—Digital Signature Certificate
ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACS	Australian Customs Service
ACSI 33	Australian Communications-Electronic Security Instruction 33
AEC	Australian Electoral Commission
AFFA	Department of Agriculture, Fisheries and Forestry Australia
ANAO	Australian National Audit Office
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
ATO	Australian Taxation Office
DEWRSB	Department of Employment, Workplace Relations, and Small Business
DHAC	Department of Health and Aged Care
DoS	Denial of Service
DSD	Defence Signals Directorate
ECI	Electronic Commerce Interface
EDI	Electronic Data Interchange
ESD	Electronic Service Delivery
GPKI	Government Public Key Infrastructure
ISP	Internet Service Provider
NOIE	National Office for the Information Economy
PKI	Public Key Infrastructure
PKT	Public Key Technology
PSM	Protective Security Manual
Treasury	Department of the Treasury

Glossary

e-commerce — (Electronic Commerce) A method of conducting or managing business- related transactions using computer and telecommunications technology.

e-mail — (Electronic mail) A facility to send messages, with or without documents or other information, electronically.

firewall — A firewall is a combination of hardware and software designed to filter information and control access to applications and data according to a set of rules.

gateway — A secured connection between an internal network and an external network such as the Internet.

gateway certification — An agency or private sector Internet gateway provider may seek an independent assessment of gateway security policy, design and management to be conducted by DSD. If successful, the gateway receives certification by DSD. A description of the *Gateway Certification Guide* may be found at Appendix 1.

Government Online (agenda) — Announced by the Prime Minister in a December 1997 policy statement *Investing for Growth*, Government Online is an initiative to see all appropriate government services deliverable via the Internet, by the end of 2001.

Internet — A worldwide public communication facility that provides an electronic pipeline for the transmission of e-mail and information between governments, businesses and individuals.

Internet browser — A software application which enables users to access the Internet.

Intrusion Detection System — A combination of hardware and software designed to monitor activity within the Internet gateway and highlight suspicious or unusual access or user activity.

Public Key Technology (PKT)
PKT is a form of cryptography that allows two parties to communicate in such a way that a third party is unable to determine the content of the message (confidentiality) or alter the message without detection (integrity). PKT can also provide authentication of identity and non-repudiation in online transactions.[1]

Public Key Infrastructure (PKI)
PKT is supported by an administrative or trust framework with standards and rules, collectively called the PKI. This framework includes PKT products, service facilities, policies, procedures, agreements and participants.[2]

router
A piece of hardware used to direct Internet traffic into and out of an Internet gateway. A router might be considered as the ‘front door’ to an agency’s Internet gateway.

[1] Consultation Paper—Privacy Issues in the Use of Public Key Infrastructure for Individuals, Office of the Federal Privacy Commissioner, June 2001, paragraph 3.1, p. 30.

[2] ibid. paragraph 3.5, p. 32.

Summary and Recommendations

Summary

Background to the Audit

1. E-Government is the use of Internet technology to enhance the access to and delivery of government services to benefit citizens, government's business partners and employees. Using the Internet to complement traditional means of service delivery, such as written communication, telephone, fax and counter services, provides greater scope for citizens and businesses to access government services in a timely and efficient manner. *Government Online—The Commonwealth Government's Strategy*[3] highlights some of the benefits to be gained by a greater use of the Internet. For many areas in government, the online environment will enable better program outcomes, such as improved service delivery options to rural and regional communities. In addition, government service delivery agencies will be able to take advantage of economies of scale presented by the online environment. For example, the Australian Job Search Internet site contains every job listed with every network member across the country, together with vacancies in the Commonwealth, those advertised in selected newspapers and some lodged directly by employers.

2. With greater agency reliance on e-Government to deliver programs and services, additional risks arise in relation to the confidentiality, integrity and availability of Commonwealth information systems and data holdings. Commonwealth agencies should ensure the security of those assets, and win and maintain the confidence of Australian citizens, businesses and government business partners if they are to successfully deliver programs and services using the Internet.

3. In moving to achieve the Government's objective of having all appropriate government services deliverable via the Internet by December 2001, (otherwise known as the *Government Online* objective) many Commonwealth departments and agencies expect to significantly increase the range, volume and complexity of services currently delivered via the Internet. *Government Online* also seeks to establish electronic payment as the normal means for Commonwealth payments and procurement. Agencies are expected to acquire or develop the capability to support secure and reliable electronic payment systems.

[3] Published by the Department of Communications, Information Technology and the Arts in April 2000, *Government Online—The Commonwealth Government's Strategy* outlines Government objectives in relation to expanding the use of the Internet by Commonwealth agencies.

4. Given the high level of activity evident in many agencies moving to progress the achievement of *Government Online* objectives, the ANAO considered it timely to review the planning, management and outcomes of Internet security measures through a performance audit. ANAO expects the results of the technical analyses of selected Internet sites to be of immediate benefit to the particular agencies concerned. At another level, the audit was intended to identify general trends in the management of Internet security by Commonwealth agencies, including better practice, and to make this information available to all agencies.

The Audit

Audit objective

5. The principal objective of the audit was to form an opinion on the adequacy of Commonwealth agencies' management of Internet security. In order to achieve this objective, the audit addressed:

- Internet security risk assessments, policies and plans;
- agencies' Internet security management procedures, to determine whether these are consistent with relevant Commonwealth guidelines and requirements, and with examples of industry better practice;
- Internet site management, including virus protection and detection strategies, prevention and detection of unauthorised access and incident response arrangements; and
- test performances of selected sites.

Audit scope

6. Together with a focus on the management systems surrounding the provision of Internet security, the ANAO considered that a comprehensive audit should also cover technical aspects of Internet security.[4] The ANAO therefore conducted this audit with the assistance of the Defence Signals Directorate (DSD). The role of the DSD team was to contribute the technical knowledge required in order to complete the audit and to test the security of selected Internet sites.

7. Ten agencies were selected to provide a broad coverage of small and larger agencies, outsourced and in-house IT management, data holdings of both personal and organisational information and agencies

[4] The audit primarily addressed the management of external security threats associated with agency use of the Internet. It was not within the scope of the audit to include a consideration of the management of security threats, the likelihood of fraud or inappropriate use of Internet facilities by staff internal to the agencies.

operating static and transactional websites[5]. The audit specifically addressed agency websites, provision of Internet e-mail and provision of Internet browser services.

8. The 10 participating agencies were:

- Australian Bureau of Statistics;
- Australian Competition and Consumer Commission;
- Australian Customs Service;
- Australian Electoral Commission;
- Australian Radiation Protection and Nuclear Safety Agency;
- Australian Taxation Office;
- Department of Agriculture, Fisheries and Forestry;
- Department of Employment, Workplace Relations and Small Business;
- Department of Health and Aged Care; and
- Department of the Treasury.

Audit Methodology

9. The ANAO reviewed the policy framework and implementation strategies of each agency and, together with DSD, selected a number of firewalls, web servers and mail servers for detailed technical examination[6]. As a large agency might operate upwards of 30 websites on a dozen or more servers, a subset of these was chosen to provide a broad sample of such activity within the agency. In total, 53 devices were examined across the 10 participating agencies. The results of the technical tests relate only to the firewalls, web servers and mail servers actually assessed, and may not directly apply to all Internet based services within an agency. Therefore, the audit findings, framed on the basis of these results, apply only to the sites tested. Nevertheless, it would not be difficult for agencies to establish whether there are wider ramifications of the results for these operations.

[5] A website described as ‘static’, usually provides information about an agency and its products or services. It is essentially a collection of documents which can be viewed and perhaps down loaded by a user. ‘Transactional’ websites support a greater degree of interaction between the user and the resources available at the website. They often support financial transactions, such as a user buying products by providing their credit card details via the website, or involve the transmission of personal or commercially sensitive information.

[6] A firewall is a specialised software package installed on a computer (a server), designed to manage and control the flow of information from one computer network to another. Firewalls, web servers and mail servers usually involve both a hardware and software component. A sound security practice is to install firewall software on a dedicated computer. That is, a computer which serves no function other than hosting essential firewall software. Web server software often resides on computers which also host the website content and web-based applications. Software for e-mail and virus protection typically resides on a mail server. In some small installations, mail server software and web server software may reside on the same computer.

10. In order to safeguard the security arrangements of the agencies assessed, this report does not present details of specific security vulnerabilities identified during the audit. Rather, the report discusses general classes of identified vulnerability and notes any trends observed across agencies. Detailed technical findings were conveyed to the agencies concerned along with recommendations to remedy any vulnerabilities detected during site testing.

11. An issues paper was presented to each of the agencies participating in the audit. The issues paper consisted of an assessment of the management systems employed by the agency and the results of site testing for each of the websites selected. The 10 issues papers contained a total of 124 recommendations; 27 recommendations relating to security policies, plans and management systems supporting the achievement of IT security policy objectives, and 97 recommendations were of a technical nature.

12. The fact that 97 technical recommendations were made does not mean that 97 exploitable vulnerabilities were identified during this audit. Many of these recommendations were aimed at increasing existing security levels. That is, they were intended to make a relatively secure installation even more secure and to promote the use of better practice in web server configuration and management.

13. The technical recommendations addressed a wide range of issues, including:

- the desirability of removing sample code, files and directories from web servers, usually installed during a 'default installation'[7] of operating system or web server software;
- the desirability of removing unnecessary applications, services and drivers from web servers;
- the configuration of particular firewalls;
- the desirability of disabling shares on web servers;[8]

[7] Software manufacturers often package software with 'default' or 'standard' settings. If the user accepts the default settings when installing the software, typically the software is installed with the maximum level of functionality. This often includes the installation of non-essential components, which may contain vulnerabilities.

[8] Many operating systems enable sharing of information by allowing a user to access other disks on the same computer, or disks on other computers on a network. If one computer is compromised this could represent a vulnerability to others on a network, through the use of these 'shares'.

- improved logging of important information and the desirability of analysing logs to help identify security issues;[9]
- improved secure coding practices for 'active content';[10] and
- the need to apply security patches in a timely manner.[11]

14. The recommendations relating to management systems encouraged agencies to:

- conduct risk assessments in relation to the additional risks associated with connecting to the Internet or providing enhanced online services;
- update or improve the relevance of security policies, particularly in relation to Internet security;
- develop (Internet) security plans, where these did not exist;
- ensure the consistent application of online security control measures; and
- develop management systems or procedures to monitor and improve compliance with elements of an agency's security policy.

15. Each agency provided a written response to ANAO in relation to the recommendations. All agencies agreed with the recommendations or agreed with some qualification, in which case further discussions were held and additional technical advice provided by DSD. Agencies informed the ANAO that the majority of these recommendations have now been implemented.

16. A small number of recommendations encouraged agencies to embark upon a course of action extending over several months. The agencies concerned have informed the ANAO of their intention to implement these recommendations.

[9] Computers are capable of recording details of user access, specific events and processes. This information is stored in 'log files.'

[10] Transactional websites are often supported by 'active content'. This usually refers to a web based application (a piece of software stored on the web server) which responds to user input, for example, providing access to a database, access to another application on the webserver or generating an e-mail message.

[11] When a vulnerability in a piece of software such as a component of an operating system or web server software is identified, the software manufacturer often releases a 'security patch'—a small piece of software designed to fix the vulnerability or at least render the vulnerability non-exploitable.

Overall Conclusion

17. The ANAO and DSD concluded that security levels across the audited agencies varied significantly from very good to very poor. For the majority of agency websites in the audit, the current level of Internet security is insufficient, given the threat environment and vulnerabilities identified within a number of agency sites. Further, while some agencies had produced good threat and risk assessments and documentation generally, these were not always effectively administered. Overall, a number of agencies could improve performance in some key areas and all agencies could improve performance in one or more aspects of managing Internet security.

18. Generally, agencies approach the management of Internet security in a way that is broadly consistent with Commonwealth policy directions, promoted in the Commonwealth Protective Security Manual and the Australian Communications—Electronic Security Instructions–33.

19. ANAO noted that most agencies had adopted a risk management approach to the management of Internet security and that, in most cases, this integrated well with the agencies' top-level risk management activities.

Key Findings

20. *ANAO found that six of the 10 agencies audited had adequately conducted and documented a risk assessment addressing the three elements of their Internet presence—website, e-mail and Internet browser access.*

21. One agency had conducted an adequate risk assessment for e-mail and browser services but had failed to conduct a risk assessment for the hosting of the agency website. Another had only identified risks associated with e-mail. Yet another agency had conducted risk assessments addressing the three elements, but the documentation relating to two of the three elements, e-mail and browser services, was significantly out of date. Only one agency had failed to conduct a risk assessment or to formally assess the risks associated with any element of its Internet presence.

22. *Small agencies tended to maintain simple sites whereas the larger agencies tended towards more complex sites. A distinction was observed between the risk management approach of smaller and larger agencies.*

23. A general observation was that small agencies maintained fairly simple websites, providing information and publications intended for public access, and that they adopted a less formal and less comprehensive approach to managing the risks associated with their Internet presence. Larger agencies tended to maintain more complex websites, with greater functionality and higher levels of user interaction. It was evident during the audit that these latter agencies adopted a more formal, well documented and comprehensive approach to managing Internet security.

24. *ANAO found that all agencies had prepared an IT security policy, as required by the Protective Security Manual, but that these varied in quality and the extent to which they referred to an agency's Internet presence.*

25. Once again, a distinction between smaller and larger agencies was noted. Larger agencies usually prepared a set of policy and operational documentation specifically for their Internet related services. Smaller agencies usually included reference, sometimes scant, to Internet services in a single document intended to cover all aspects of IT security for the agency.

26. *ANAO found that only the larger agencies, particularly those that managed their Internet presence using in-house resources, developed comprehensive security plans, disaster recovery or business continuity plans.*

27. Agencies managing Internet security in-house demonstrated a more holistic and comprehensive approach to documenting plans and security strategies. Agencies outsourcing delivery of some elements of their Internet presence demonstrated a more fragmented, and often incomplete, set of planning documentation. In some cases, where an external service provided had been contracted to provide secure Internet gateway services, the provider had developed security and business continuity plans in consultation with the relevant agencies.

28. *ANAO noted a high degree of correlation between the perceived level of risk associated with an agency's Internet presence and the apparent effort devoted to risk identification, risk assessment and risk control strategies.*

29. That is, an agency with a relatively static website and no connection between the website and the agency's internal computer network, usually assessed the risks as low and devoted relatively little attention to actively managing Internet security. On the other hand, larger agencies with relatively sophisticated websites, supporting transactions with customers and clients, devoted significantly more resources to actively managing the perceived higher levels of risk.

30. *Agencies operating websites that involved the transmission of personal information or sensitive commercial information between clients and an agency were, in general, found to pay adequate attention to protecting the privacy of the individuals concerned.*

31. ANAO noted that six of the 10 agencies operated relatively static websites, while the other four operated websites which supported transactions with members of the public or the business sector. The four agencies operating transactional websites did so using in-house resources, or in one case using a mixture of in-house resources and the agency's IT outsourcing partner.

32. *ANAO found considerable variation in the quality and appropriateness of contracts supporting the outsourcing of website hosting and, occasionally, other elements of an agency's Internet presence.*

33. Some contracts examined by ANAO failed to specify expected service levels or lacked reference to clear performance indicators. ANAO concluded that such circumstances reduced the agency's ability to effectively manage the contract and that, in some instances, key agency staff were unaware of the security measures delivered by their external service providers.

34. Some contracts examined during the audit contained nothing, or very little, by way of provision for agency staff to audit the security provisions of their service providers. In contrast, ANAO noted that a number of contracts not only provided for agency staff to audit contractors' security arrangements but that provision was also made for the Auditor-General or the Commonwealth Privacy Commission to audit security and privacy practices employed by contractors.

35. *Selected Internet sites were tested by staff from the Defence Signals Directorate (DSD). Six of the 10 agencies audited were found to manage websites containing significant vulnerabilities, potentially exploitable by a malicious user over the Internet. In addition, the audit team identified other security issues in all sites.*

36. Test results indicated that, generally, agencies were making good use of technology such as routers and firewalls to establish effective perimeter security for their websites. The audit team noted that the quality of web server and mail server configuration was variable, with a number of servers running unnecessary software, which could represent vulnerabilities in an otherwise secure configuration.

37. When a software 'bug' or exploitable vulnerability is discovered, the software vendor may release a security patch; additional software designed to make the vulnerability non-exploitable. The audit team identified the lack of a procedure promoting the timely application of security patches as a major shortcoming in the majority of agencies.

38. *Where Commonwealth websites were hosted and managed using in-house resources, the level of co-ordination and communication between relevant groups was substantially better than when site management was contracted to an external service provider.*

39. This is not to say that security outcomes are necessarily better, simply that substantially more effort is required to manage the relationships between key players in an outsourced environment.

40. *Where intrusion detection systems were employed, usually in fairly large and complex Internet gateways, these were generally well-managed and represented a strong addition to the overall security of the gateway.*

41. *Nine of the 10 agencies had implemented anti-virus products appropriately.*

42. Most commonly, different anti-virus products from different software vendors were employed at different points in the agency's network and Internet gateway. In this way, the breadth of coverage afforded an agency is greater than that afforded by the use of a single anti-virus product. One agency was found to have very poor practices in relation to using anti-virus software. Users were able to, and did, disable the desktop installation of the anti-virus software, thereby rendering any protection against viruses ineffective.

43. *The testing program revealed that policy and procedures for the review of audit logs was very poor. This highlights the importance of agencies auditing security logs to manage threats.*

44. Most web servers generate access logs and event logs. The audit team found that those agencies that regularly examined these logs were better placed to manage threats associated with unusual or suspicious activity over the Internet.

45. *Better performing agencies in this audit had comprehensive knowledge of their systems, clearly defined responsibilities for key players, an active approach to maintaining security and the ability to respond quickly to issues and incidents as they arise.*

Recommendations

46. As noted earlier, issues papers, including specifically tailored recommendations, were presented to each of the agencies in June 2001. Each agency provided a written response to ANAO in relation to the recommendations and all agencies agreed with the recommendations. Agencies informed the ANAO that action on many recommendations had been completed by the end of July 2001.

47. ANAO and DSD assessed the broad classes of vulnerability observed across the 10 agencies and addressed, where necessary, in the recommendations specific to the audited agencies. This resulted in ANAO and DSD synthesising a core of general recommendations applicable to all Commonwealth agencies with an Internet presence. Comments received by the ANAO from the participating agencies, reflect widespread acceptance of these general recommendations.

The following recommendations have general application to all agencies:

- **Agencies should adopt a structured approach to the management of Internet security, employing a sound risk management model.** This is reinforced in the Commonwealth's published policy on information security;
- **Agencies should ensure that appropriate risk assessments are conducted.** Prior to introducing a new IT system, web based application or instituting a major change to current online services, a risk assessment should be undertaken to identify any new or untreated risks;
- **Agencies should avoid default installations of operating system and web server software.** These systems should be 'security hardened'[12] by removing unnecessary services and functionality which could represent risks to the integrity of the web servers;
- **Agencies should test and install security patches in a timely manner.** Knowledge of particular vulnerabilities spreads quickly on the Internet, and many hackers target recent vulnerabilities in the hope that web server administrators have not installed the relevant security patches;

[12] Most software manufactures publish checklists and other guidance material on how to harden web servers. DSD and NOIE may also be able to provide assistance in relation to sourcing guidance material for particular operating systems and varieties of web server software.

- **Security administrators should regularly review logs.** Access logs and event logs are a rich source of information for the web server administrator. Analysing these logs may provide considerable insight into the usage patterns of a website and highlight suspicious or unusual activity;
- **Agencies should ensure that applications which support transactions with users, such as active content, are reviewed for secure coding practices.** Having such code reviewed by a third party, i.e., someone not involved in writing or implementing the code, enhances the level of security associated with the application; and
- **Agencies should ensure that relevant documentation is kept up to date.** Security documentation (such as policies, plans and network descriptions) is of most use to security administrators when it is comprehensive and kept up to date.

48. The Commonwealth Protective Security Manual (PSM) and the Australian Communications–Electronic Security Instructions–33 (ACSI-33) provide guidance to agencies on managing risks to the security of Commonwealth information and Information Technology assets. The PSM identifies a set of minimum standards intended to bind all Commonwealth agencies and employs a six-step model to illustrate the key stages of a security risk management process. ACSI-33 provides practical advice on how to apply the PSM model to protect information systems.

49. The National Office for the Information Economy (NOIE) has published a *Guide to Minimum Website Standards*.[13] The ANAO Better Practice Guide *Internet Delivery Decisions*[14] provides a useful framework for public sector managers to employ when considering the Internet as a program delivery mechanism.

[13] Available at the NOIE website—www.noie.gov.au

[14] Available at the ANAO website—www.anao.gov.au, and in hard copy, from the ANAO Publication Unit.

50. Part 6 of the ANAO Better Practice Guide, Internet Systems Security and Authentication for Government Programs, was prepared by NOIE and DSD. It contains a set of resources designed to assist in the implementation of effective Internet security strategies. These resources, including a 'Website and Internet System Security Checklist', are organised around four main themes:

- **protection** of Commonwealth online systems and information assets;
- **detection** of incidents and vulnerabilities;
- **reaction** to address and resolve online security issues or incidents as they emerge; and
- **authentication** of the parties to online transactions.

Audit Findings and Conclusions

1. Introduction

This chapter outlines some of the drivers and risks associated with government connecting to the Internet. It describes the policy framework intended to ensure the security of Commonwealth information assets, particularly in relation to managing Internet security, and it concludes with a description of the audit approach.

Government Agencies on the Internet

1.1 A high proportion of Australians access the Internet compared to proportions of users in most other countries. At May 2000, 6.4 million adults (46 per cent of all Australian adults) accessed the Internet from home, work or some other site.[15] The Australian Bureau of Statistics estimates that by the end of 2001, over half of all adult Australians will use the Internet on a regular basis.

1.2 At February 2000, the proportion of small and medium businesses online in Australia was 60 per cent[16]. As Australian citizens and businesses become increasingly 'Internet enabled', they will require greater access to a wider range of electronic services, including government services.

1.3 The Commonwealth Government has recognised the importance of these developments. The *Government Online* strategy pursues a commitment that all appropriate Government services will be available, via the Internet, by the end of 2001.[17] In pursuit of this commitment, and for the Government to take full advantage of the potential of the information age, the Government has assigned to the National Office for the Information Economy (NOIE)[18] the key role of promoting and supporting community, business and government use of the online environment.

[15] *Use of the Internet by Householders, Australia, May 2000 (8147.0)* Australian Bureau of Statistics, November 2000.

[16] The Yellow Pages and the National Office for the Information Economy, Small Business Index, June 2000.

[17] Announced in the Prime Minister's *Investing for Growth* statement, December, 1997.

[18] An Executive Agency within the Communications, Information Technology and the Arts Portfolio.

1.4 At December 2000, over 90 per cent of Commonwealth Government departments and agencies had established an Internet presence.[19] The nature of this Internet presence varies significantly between agencies. A number of these sites are static, that is, they simply provide information about an agency and its products or services. Other agency Internet sites facilitate transactions between the agency and the business sector or between the agency and individuals. These transactions can be financial or involve the transmission of personal or commercially sensitive information.

1.5 In moving to achieve the *Government Online* objective, many Commonwealth departments and agencies expect to significantly increase the range, volume and complexity of services delivered via the Internet.

1.6 E-Government is the use of (Internet) technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees[20]. Using the Internet to complement traditional means of service delivery, such as written communication, telephone, fax and counter services, may allow more citizens and businesses to access government services in a timely and efficient manner. *Government Online—The Commonwealth Government's Strategy*[21] highlights some of the benefits to be gained by a greater use of the Internet. For many areas in government, the online environment will enable better program outcomes, such as improved service delivery options to rural and regional communities. Government service delivery agencies will be able to take advantage of economies of scale presented by the online environment.

1.7 For example, the Australian Job Search Internet site contains every job listed with every network member across the country, together with vacancies in the Commonwealth, those advertised in selected newspapers and some lodged directly by employers. The Internet is clearly an efficient means of providing access to the largest employment database in the country. Attempting to maintain up to date collections of such information in hard copy, in multiple service delivery centres across the country, would be much less efficient.

[19] *Commonwealth Government Online - Progress Report,* NOIE, December, 2000.

[20] At the Dawn of e-Government, Deloitte Research, 2000, p. 1.

[21] Published by the Department of Communications, Information Technology and the Arts in April 2000, *Government Online—The Commonwealth Government's Strategy* outlines Government objectives in relation to expanding the use of the Internet by Commonwealth agencies.

1.8 With greater agency reliance on e-Government to deliver programs and services, additional risks arise in relation to the confidentiality, integrity and availability of Commonwealth information systems and data holdings. Commonwealth agencies should ensure the security of those assets, and win and maintain the confidence of Australian citizens and business partners if they are to successfully deliver programs and services using the Internet.

What are the risks associated with the Internet?

1.9 The number of Internet related security incidents reported annually, in Australia and overseas, is steadily rising[22]. These incidents occur for several reasons. Computer hackers attempt to exploit vulnerabilities in operating systems, applications and communications protocols to gain unauthorised access to information and to take control of IT systems. Some hackers operate without malicious intent, breaking into systems to satisfy their curiosity or to test their programming skills. Others clearly breach IT systems with malicious or criminal intent and can inflict significant damage on their victims. Damage may range from the embarrassment of website defacement, to the compromise or unauthorised release of information and the use of the compromised computer in the perpetration of other crimes.

1.10 Computer viruses are probably the most widely known Internet security threat. The introduction of viruses or other malicious code can impact significantly on IT systems and the information processed and stored on those systems. The scale of damage may range from a slight reduction in system performance to total loss of data, applications and operating systems.

[22] The Australian Computer Emergency Response Team (AusCERT), part of a global network of computer security incident response teams, collects statistics on Internet security. The trend is clearly that of a rapid increase in the number of security breaches over recent years. Caution must be exercised in interpreting these data since part of the apparent increase in the number of Internet security incidents may be a result of improved reporting practices.

Internet security incidents reported in Australia - 1996-2000. AusCERT, 2001

Year	1996	1997	1998	1999	2000
Incidents	309	572	1 342	1 816	8 197

The CERT Coordination Centre reports security incident statistics for the USA.

Internet security incidents reported in USA - 1996-2000. CERT/CC, 2001

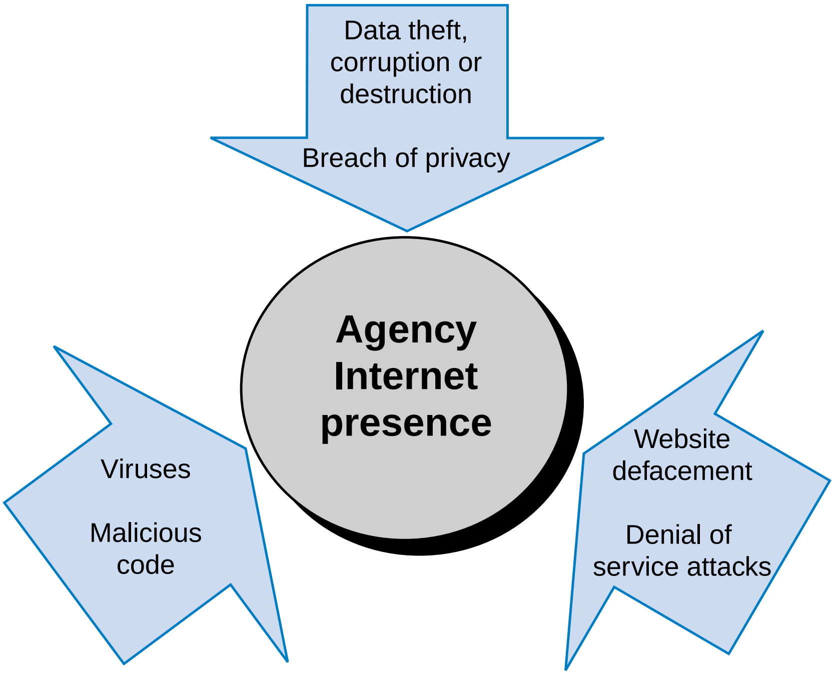
Year	1996	1997	1998	1999	2000
Incidents	2 573	2 134	3 734	9 859	21 756

1.11 Government agencies using the Internet also have the risk of a denial of service attack. In its simplest form, a denial of service (DoS) attack aims to disrupt a computer network by overloading it with useless communications traffic. The effect is to deny services to legitimate users. Distributed denial of service attacks use the resources of previously 'infected' or hacked computers to launch denial of service attacks from many such machines against a small number of targets. A DoS attack may be prolonged and cause web servers to be shut down entirely. The realisation of any of these threats is likely to result in at least a temporary reduction of service to government customers.

1.12 E-commerce presents another set of risks associated with fraudulent activity, identity theft or the theft of credit card numbers. Threats also exist to personal privacy, the compromise or unauthorised publication or release of clients' personal information. While Commonwealth departments and agencies have for some time been required to comply with privacy legislation and guidelines, recent amendments to the *Privacy Act 1988* will see many provisions of the Act apply to large corporations in the private sector from 21 December 2001. Such changes are reflective of the increased attention paid to ensuring adequate controls over the use of personal information in any business context, not just a government business context.

Figure 1

Major risks associated with hackers, malicious or unauthorised users accessing agency information via the Internet.



1.13 In an unclassified, public version of a report on the threats and vulnerabilities to Australia's Information Infrastructure[23], the Defence Signals Directorate reached a number of important conclusions, including:

- viruses and hacking will continue to be the major threats to software and information in the foreseeable future;
- the rate of hacking is expected to increase in proportion to the increase in computer literacy and Internet connectivity;
- the skill level of hackers generally is expected to increase, in large part due to the ready availability of hacking techniques on the Internet; and
- deliberate threats are increasing and will continue to do so.

Commonwealth departments and agencies connected to the Internet are subject to these risks daily.

Threats to Commonwealth Agencies using the Internet

1.14 Where an agency delivers services that are essential to the well-being of many Australians, such as Centrelink delivering welfare programs, or where an agency maintains a substantial holding of personal or commercial information, such as the Australian Taxation Office data holdings, the impact of non-delivery of services or confidential information becoming public can be far reaching and affect a large number of Australian businesses and individuals.

1.15 If a Commonwealth agency, like any entity operating on the Internet, is not aware of the potential risks and does not have appropriate management procedures and policies in place to deal with the risks and any related incidents, it could potentially cause a severe financial, social and political disruption.

1.16 Australian citizens accessing government services via the Internet need to have confidence in the security of their transactions with government departments. They need to feel that their personal privacy is protected. They need to know that government services accessed via the Internet will deliver equivalent outcomes to other forms of program delivery, such as visiting a government office or accessing services via the telephone.

[23] Protecting Australia's National Information Infrastructure—Report of the Interdepartmental Committee, Attorney-General's Department, Canberra, Attachment A (DSD report), Feb 1997.

1.17 Agencies employing effective security measures and well designed Internet sites are best placed to provide those assurances to their clients and customers. On the other hand, if an agency employs Internet technology in such a way that its programs are delivered poorly, at a higher cost or in an insecure manner, Australian citizens and businesses are likely to lose confidence and respond negatively to the e-Government initiative.

1.18 It is important to note that the nature of information technology, the software, hardware and communication protocols used, combined with the rapid rate of change in the Internet environment act against achieving absolute security within that environment. It is not possible to achieve a '100 per cent secure' Internet presence.

1.19 It is possible, however, to identify and assess the risks associated with conducting government business via the Internet and to implement control measures designed to provide an acceptable level of security and to manage any residual risk. Constant vigilance is necessary as an IT security manager may work to address every known vulnerability applicable to his or her system at one point in time, yet remain open to a newly created vulnerability.

Risk management

1.20 The challenge for Commonwealth departments and agencies, then, is that of effective risk management. While connecting to the Internet may represent a new and somewhat different set of risks, Commonwealth departments and agencies have traditionally been required to manage the security of Commonwealth information assets, whether they are stored electronically or otherwise.

1.21 Management of these risks can be undertaken through a variety of means though some elements consistently arise in better practice models. These include:

- the conduct of threat and risk assessments for the agency's Internet presence;
- the development of Internet gateway security policies and plans;
- detailed incident response and business continuity planning;
- incorporating reporting mechanisms into management systems;
- raising staff awareness and delivering appropriate training; and
- identifying staff responsible for the management and implementation of security measures.

1.22 Such management tools may be employed within a variety of organisational structures and situations to effectively manage the risks associated with the Internet. The ANAO recognises that a significant number of Commonwealth departments and agencies have outsourced the provision of their IT infrastructure. The Commonwealth Protective Security Manual supports the view that while an agency or department may deem this a sound management decision, ultimately the responsibility for the security of Commonwealth information remains with the relevant Secretary or Chief Executive Officer. The function may be outsourced, the responsibility may not.

1.23 Agencies or departments that outsource part or all of their Internet presence are able to utilise the same management tools as those that carry out the function in-house. In this situation, management of the risks associated with an Internet presence becomes an exercise in contract management. While the policies can be created by the contractor or the agency, as the ultimate responsibility for protecting the information lies with the agency head, the agency needs to effectively manage the contractor to deliver the outputs and outcomes envisaged in policies and procedures.

Commonwealth Guidelines

1.24 The Commonwealth has published guidelines to assist agencies in managing risks to the security of Commonwealth information and IT systems. The Commonwealth Protective Security Manual (PSM) provides a framework for physical, information and personnel security. In regard to information security, there is a strong emphasis on ensuring the availability, integrity and confidentiality of Commonwealth information holdings. The PSM discusses the roles and responsibilities for security risk management and employs a six-step model to illustrate the key stages of a security risk management process. The PSM clearly identifies a set of minimum standards intended to bind all Commonwealth agencies.

These are:

- the Government expects that each of its agencies will prepare a security plan using risk management principles;
- minimum standards, whether imposed by legislation or government policy, must form part of every agency's security plan;
- each agency must establish and maintain a security environment appropriate to its functions and responsibilities; and
- the risk environment must be monitored continuously, and the security plan must be evaluated to ensure that the treatments and strategies are effective and cost efficient.

1.25 Other key Government directions include;

- the *Australian Communications-Electronic Security Instructions-33* (ACSI-33) maintained by the Defence Signals Directorate;
- the *Gateway Certification Guide, version 2.1*, maintained by the Defence Signals Directorate;
- a *Guide to Minimum Website Standards* maintained by the National Office for the Information Economy (NOIE); and
- The Commonwealth *Privacy Act 1988.*

1.26 Greater detail on the contents and requirements of these documents is provided in Appendix 1.

Previous ANAO reports

1.27 The ANAO has tabled two reports relating to Commonwealth agency's use of the Internet and published a relevant Better Practice Guide. Each of these publications has addressed Internet security issues.

The ANAO publications were as follows:

- Audit Report No.15, 1997–98, *Internet Security Management.*

  The audit report concluded that most agencies had some of the core elements required for effective Internet security management; however, improvement was required in several key areas including risk assessments, configuration and operation of firewalls, analysis of security logs and anti-virus controls.

  The key recommendations contained in the report focused on careful planning of the Internet connection, adequately documenting policies, plans and procedures necessary for secure site management and the more effective, timely use of available security tools.

- Audit Report No.18, 1999–2000, *Electronic Service Delivery, including Internet Use, by Commonwealth Government Agencies.*

  The report identified four stages in the evolution of a Commonwealth agency Internet site: provision of information about the agency, provision for users to browse and explore selected data, provision for the user to engage in secure transactions with the agency, and provision of a whole-of-government integrated service to users.

  The audit, based on a survey of 66 agencies subject to the *Financial Management and Accountability Act 1997,* concluded that most agencies were well positioned to meet the Government Online agenda of providing appropriate Government services via the Internet by 2001.

The report recommended, among other things, that individual agencies reassess their risks and related control strategies as they increase their use of the Internet and other forms of electronic service delivery mechanisms.

- Better Practice Guide, *Internet Delivery Decisions. A Commonwealth Program Manager's Guide, 2001.*

  Launched in April 2001, the Guide identifies key questions and issues for managers to consider when deciding whether, and how, to use the Internet for delivery of government services. Presented in nine parts, the guide contains a section on "Internet Systems Security and Authentication for Government Programs".

1.28 The ANAO has also tabled Audit Report No.9, 2000–01, *Implementation of Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative*, which contained some audit findings in relation to IT security in an outsourced environment.

Audit objective and scope

Audit objective

1.29 Given the high level of activity evident in many agencies moving to progress the achievement of *Government Online* objectives, the ANAO considered it timely to review the planning and management of Internet security measures through a performance audit. ANAO expected the results of the technical analyses of test Internet sites to be of immediate benefit to the particular agencies concerned. At another level, the audit was intended to identify general trends in the management of Internet security by Commonwealth agencies, including better practice, and to make this information available to all agencies.

1.30 The principal objective of the audit was to form an opinion on the adequacy of Commonwealth agencies' management of Internet security. In order to achieve this objective, the audit addressed:

- Internet security risk assessments, policies and plans;
- agencies' Internet security management procedures, to determine whether these are consistent with relevant Commonwealth guidelines and requirements, and with examples of industry better practice;
- Internet site management including virus protection and detection strategies, prevention and detection of unauthorised access and incident response arrangements; and
- test performances of selected sites.

Audit scope

1.31 While the focus of the audit was on the management systems surrounding the provision of Internet security, the ANAO considered that a comprehensive audit should also cover technical aspects of Internet security. The ANAO therefore conducted this audit with the assistance of the Defence Signals Directorate (DSD).[24] The role of the DSD team was to contribute the technical knowledge required in order to complete the audit. DSD staff were appointed under provisions of the *Auditor-General Act 1997* for the period of the audit. The DSD team performed a detailed technical examination of selected web servers, mail servers and other Internet services in each agency. An element of the technical examination involved assessing sites against a range of publicly known vulnerabilities.

1.32 There were 10 agencies included within the scope of the audit. The agencies were selected on the basis of several criteria. These included:

- agency size;
- whether the IT infrastructure of the agency was managed in-house or outsourced;
- the nature of the information held by the agency (personal or organisational); and
- the nature of the agency web site (transactional or static content).

1.33 The 10 agencies were selected to provide an insight into the management of Internet security across a broad cross-section of the Commonwealth's Internet presence. They were:

- Australian Bureau of Statistics;
- Australian Competition and Consumer Commission;
- Australian Customs Service;
- Australian Electoral Commission;
- Australian Radiation Protection and Nuclear Safety Agency;
- Australian Taxation Office;
- Department of Agriculture, Fisheries and Forestry;
- Department of Employment, Workplace Relations and Small Business;
- Department of Health and Aged Care; and
- Department of the Treasury.

[24] By Government directive in October 1986, the Defence Signals Directorate was designated as the national computer and communications security authority, and ascribed particular roles in relation to providing advice and assistance to Commonwealth departments and agencies.

1.34 The audit did not address the financial costs of Internet security, nor explore in detail the issue of human resource costs associated with managing Internet security in-house. Where these factors were observed to be important in the context of an agency's management of Internet security, they are mentioned in this report on an exception basis.

Audit methodology

1.35 Fieldwork was conducted from January to April 2001. An issues paper was presented to each agency in June 2001, outlining preliminary audit findings in respect of the individual agency's Internet security management and findings of DSD's testing of the security of each site. The results of all 10 agencies were analysed and aggregated to form the basis for this report.

1.36 All agencies agreed to co-operate with the site testing component of the audit. Those agencies that had outsourced web hosting assisted in discussions with their external service providers. In turn, this contributed to gaining the co-operation of those external service providers in the site testing component.

1.37 In consultation with the agencies concerned, ANAO and DSD selected a number of firewalls, web servers and mail servers for detailed technical examination. In some cases an agency maintained only one major website or operated only one web server, in other cases an agency might operate upwards of 30 individual websites, hosted on dozens of web servers. As it was not possible to thoroughly test all websites and Internet based services of the 10 participating agencies, DSD and ANAO sought to ensure a broad sampling of agencies' online activity for the testing phase.

1.38 Consequently, particularly in the case of larger agencies where only a sample of Internet sites were tested, any findings reported in this audit may not directly apply to the whole of an agency's Internet presence. Findings relate to the sites actually tested. Nevertheless, it would not be difficult for agencies to establish whether there are wider ramifications of the results of the operations tested during this audit. DSD examined a total of 53 firewalls, web servers and mail servers over the 10 agencies. The smallest number of devices tested in an agency was one; the greatest number tested in an agency was 12 , with the average number per agency being five.

1.39 The issues papers presented to agencies contained a total of 124 recommendations; 27 recommendations relating to security policies, plans and management systems supporting the achievement of IT security policy objectives, and 97 recommendations were of a technical nature. Each agency provided a written response to ANAO in relation to the recommendations. All agencies agreed with the recommendations or agreed with some qualification, in which case further discussions were held and additional technical advice provided by DSD. Agencies informed the ANAO that many recommendations had been implemented by the end of July 2001. In cases where recommendations required a longer period of time for full implementation, agencies informed the ANAO that action had either commenced or was planned to commence within a reasonable time.

1.40 The audit was conducted in accord with ANAO Auditing Standards at a cost to the ANAO of $280 000.

Structure of this report

1.41 This report outlines findings in relation to the audit criteria. Chapters 2–4 focus respectively on the following issues:

- Internet security risk assessments, policies and plans;
- Elements of Internet site management; and
- Internet security outcomes.

2. Internet Security Risk Assessments, Policies and Plans

This chapter presents audit findings and discusses the conduct of risk assessments and the preparation of Internet related security policies, plans and business continuity plans, by agencies involved in the audit.

Context

2.1 In 1996 the Commonwealth's Management Advisory Board and Management Improvement Advisory Committee released *MAB/MIAC Report Number 22—Guidelines for Managing Risk in the Australian Public Service*. That report outlined a general framework for risk management applicable to many elements of public administration. The management of IT systems employed by departments and agencies is one activity amenable to the application of a risk management framework.

2.2 For some years now, IT managers have been encouraged to apply a risk management approach to the design and administration of IT systems, especially those critical to achieving an agency's business objectives. Both the Commonwealth Protective Security Manual (PSM) and the Australian Communications—Electronic Security Instructions No.33 (ACSI-33) call for the application of a risk management approach to IT security.

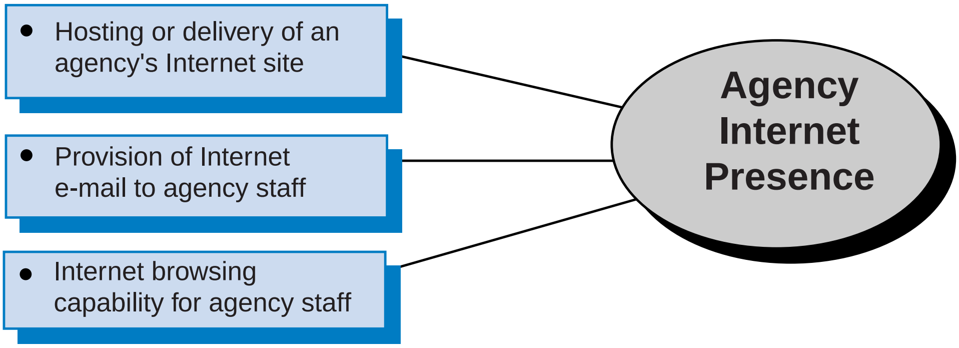
2.3 Connecting to the Internet presents an agency with an additional set of risks, many unique to that environment and some markedly different to other risks associated with managing a trusted internal computer network. Therefore, the design and management of an agency Internet presence, particularly the management of Internet security, is well served by a specific application of risk management.

2.4 Often the complexity of the agency's IT systems, or more particularly the complexity of the agency's Internet connectivity, will determine whether a specific set of risk management documentation should be generated in relation to Internet based services. For agencies with a relatively simple, and often low-risk Internet profile, it is perhaps more appropriate to include a section addressing Internet services in the agency's overarching IT systems security documentation.

2.5 Three elements of an agency's Internet presence were included within the scope of this audit. The ANAO considers that the risks associated with each should be addressed, and control measures included in an agency's IT security documentation. The three elements of an agency's Internet presence assessed during this audit were:

Figure 2

Elements of an agency's Internet presence



Hosting or delivery of an agency's Internet site
Provision of Internet e-mail to agency staff
Internet browsing capability for agency staff
Agency Internet Presence

2.6 Some agencies host their own Internet site(s), others outsource this function. Some have engaged one supplier for e-mail or browser services; others have split the functions across two external service providers. As part of the Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative, some agencies have outsourced provision and management of their IT infrastructure.

2.7 Some agency websites are hosted by their infrastructure service provider, others by another contractor specialising in the provision of Internet related services. In some cases, an agency's infrastructure service provider manages a contract with another service provider delivering Internet related services.

2.8 Some agencies provide Internet browser access to their users' desktop. This usually involves some form of controlled link between an agency's internal network and the Internet. Other agencies have taken the decision to provide Internet browser access via a series of stand-alone machines, not connected to an internal network.

2.9 When deciding to outsource e-mail, browser or website hosting services, agencies can choose from a large number of commercial Internet Service Providers (ISPs). Often, ISPs offer different levels of service and security. Some specialise in offering secure Internet services to government customers, and in an effort to attract such customers have sought certification of their Internet gateway by DSD. Six of the 10 agencies participating in this audit had engaged the services of one such DSD certified gateway provider,[25] for one, two or all three elements of their Internet presence.

2.10 The following Table summarises outsourcing arrangements for the 10 agencies. Where an agency has entered into arrangements with multiple service providers this is illustrated by indicating 'provider No.1', 'provider No.2' .. etc. The DSD certified gateway provider referred to in the preceding paragraph is indicated in bold type.

Table 1

Summary of outsourcing/contracting arrangements in participating agencies

Agency	*Agency IT Infrastructure*	*Internal network connected to Internet*	*Internet site hosting*	*Internet E-mail*	*Internet Browser access*
ABS	In-house	e-mail and restricted browser access	In-house	In-house	In-house
ACCC	Outsourced provider No. 1	Yes	Outsourced provider No. 2	Outsourced **provider No. 3**	Outsourced **provider No. 3**
ACS	Outsourced provider No. 1	e-mail only	Outsourced Subcontracted by provider No. 2 to provider No. 3	Outsourced **provider No. 4**	Outsourced Subcontracted by provider No. 2 to provider No. 3
AEC	Outsourced provider No. 1	Yes	Outsourced provider No. 1	Outsourced provider No. 1	Outsourced provider No. 1
AFFA	Outsourced provider No. 1	Yes	Outsourced **provider No. 2**	Outsourced **provider No. 2**	Outsourced **provider No. 2**
ARPANSA Scinet- Corporate	In-house Through DHAC	Yes Yes	In-house **Through DHAC**	Outsourced provider No. 1 **Through DHAC**	Outsourced provider No. 1 **Through DHAC**
ATO	Outsourced provider No. 1	Yes	In-house, in partnership with provider No. 1	Outsourced provider No. 2	Outsourced **provider No. 3**
DEWRSB	In-house	Yes	In-house	In-house	In-house
DHAC	Outsourced provider No. 1	Yes	Outsourced **provider No. 2**	Outsourced **provider No. 2**	Outsourced **provider No. 2**
Treasury	In-house	Yes	In-house	In-house	In-house

[25] DSD has certified some individual gateways that are managed by ISPs. It should be noted that DSD certification extends to a particular gateway, not a provider. A standard DSD gateway certification does not cover the configuration of web servers.

2.11 The Table shows that:

- four of the 10 agencies managed their IT infrastructure with their own staff, and six agencies, in whole or in part, outsourced management of their IT infrastructure;
- eight of the 10 agencies connected their internal computer networks to the Internet, and two agencies did not, preferring to connect to the Internet on machines which had no function other than to provide Internet browser services;
- three agencies hosted their Internet site(s) using their own hardware and software, two agencies hosted their Internet site(s) using a combination of their own and a provider's resources, while five agencies contracted providers to host their Internet site(s);
- six agencies use a DSD certified gateway provider for at least one element of their Internet presence, while three of the 10 agencies use the DSD certified gateway for all three elements of their Internet presence.

Description of Internet sites assessed in this audit

2.12 A brief description of the Internet sites assessed during this audit appears below. Many of these sites present a diverse range of information and services. Only some of the key features are highlighted in the following description, in order to give the reader a general understanding of the government programs and services delivered by these sites.

Australian Bureau of Statistics—www.abs.gov.au

2.13 The ABS site allows users to access the entire ABS standard product range (AusStats). The range includes a statistical profile of Australia, all ABS publications from 1998 onwards, spreadsheets containing economic and social data and an ABS on-line catalogue. AusStats comprises hundreds of standard reports. Users are not permitted to access or interrogate the underlying databases.

2.14 The site also highlights recent publications and additions to the AusStats service as well as presenting information about the Bureau, the census, news and recruitment opportunities with ABS.

2.15 ABS operates a subscription service through which customers may access statistical reports, prepared on a regular basis, through a fee for service arrangement.

Australian Competition and Consumer Commission—www.accc.gov.au

2.16 The ACCC site contains a variety of information in the form of publications, media releases and speeches on matters relevant to the agency and its work. Along with information about ACCC, recruitment and contact details, the site allows users to contact ACCC via Internet e-mail.

2.17 One particular feature of the site, Slam-a-Cyberscam, provides users with the ability to report instances of individuals or companies allegedly employing illegal or suspect business practices utilising the Internet. Users complete a series of electronic forms on-line and submit the information to ACCC, essentially as e-mail.

Australian Customs Service—www.customs.gov.au

2.18 Customs' site presents users with information about the Australian Customs Service, media releases and publications and Customs Notices. The site provides guidance on importing goods into Australia, Customs Tax Reform and Cargo Management Reform. The site permits users to contacts Customs and communicate complaints and compliments.

Australian Electoral Commission - www.aec.gov.au

2.19 The AEC website contains media releases, publications and information about the Electoral Commission. Users may access documents relating to electoral education, Australian electoral history, past elections, referendums and legislation.

2.20 The site also contains information on voting, enrolment, electorates and party registration. The site contains a number of links to other electoral sites and further information on international electoral services.

Department of Agriculture, Fisheries and Forestry Australia - www.affa.gov.au

2.21 The AFFA website provides users with access to a wide range of publications and news on matters of topical interest. Resources on foot and mouth disease, ovine Johne's disease and mad cow disease are present, along with information on biosecurity, Agriculture Advancing Australia, a national action plan for salinity and water control and "Agribiz".

2.22 The site links to information for AQIS, the Australian Quarantine Inspection Service, ABARE, the Australian Bureau of Agricultural and Resource Economics, and BRS, the Bureau of Rural Sciences.

Australian Radiation Protection and Nuclear Safety Agency - www.arpansa.gov.au

2.23 ARPANSA’s site contains the agency’s service charter and information on the agency’s role and function as well as the services it provides. Radiation and Health News, UV Resource Guide and the provision of draft documents for public comment are among the publications accessible by users. ARPANSA’s main site is hosted within the environment of the Department of Health and Aged Care.

2.24 The agency operates a second website, hosted on a separate network. The second network, used in connection with some ARPANSA business functions including scientific research undertaken by ARPANSA, was the primary subject of this audit.

Australian Taxation Office - www.eci.ato.gov.au

2.25 The ATO hosts a large number of Internet sites. The site assessed during this audit was the ATO’s Electronic Commerce Interface (ECI). This site serves as a gateway for businesses to lodge a Business Activity Statement (BAS) electronically. It therefore deals with the transmission of personal and commercially sensitive information, between individuals and the ATO.

2.26 This particular site employs Public Key Infrastructure (PKI) to encrypt data and secure the transactions as well as providing a means of authenticating users. ECI involves client software which allows Australian businesses with an Australian Business Number, to collect documents from the ATO electronically, check documents for errors before sending and to send documents electronically to the ATO.

Department of Employment, Workplace Relations and Small Business - www.business.gov.au

2.27 DEWRSB hosts a number of websites. The site chosen for assessment in this audit was the Business Entry Point (BEP) site. Through the Australian Business Register, this site allows Australian individuals and businesses to apply online for an Australian Business Number (ABN). It deals with the transmission of personal and business information.

Department of Health and Aged Care - www.health.gov.au

2.28 DHAC’s main website contains a range of publications, media releases and speeches as well as linking to information on immunisation, health insurance, residential aged care resources, the national alcohol campaign and national illicit drugs campaign and the Health*Insite* resource.

2.29 DHAC operates a number of other subject-specific websites, such as those supporting the quality use of medicines, specific youth services and topical public health issues. Some of these sites were assessed during the audit.

Department of the Treasury - www.treasury.gov.au

2.30 The Treasury site provides users with access to a range of publications about the functions of the Treasury, consumer affairs, economic data, business taxation and foreign investment. The site also contains information on recruitment, press releases, speeches and contact details and links to the Commonwealth budget Internet site and sites for the Treasury Ministers.

Risk assessments

2.31 Whether an agency incorporates an Internet component into its agency IT security documentation or develops a specific set of documentation for its Internet presence, a fundamental first step is the conduct of a risk assessment.

2.32 Risks exist to the confidentiality, integrity and availability of Commonwealth information. The following Table summarises the major risks associated with connecting internal networks to the Internet.

Table 2

Risks to confidentiality, integrity and availability of Commonwealth information

CONFIDENTIALITY	*INTEGRITY*	*AVAILABILITY*
• Theft of data stored on a website, but not intended for public access (e.g. databases or files supporting some functionality of the website). • Unauthorised access to data stored on an agency's internal network (if the network is connected to the Internet). • Unauthorised release of personal or commercially sensitive information.	• Destruction or corruption of information stored on a website, including a defacement of the website. • Destruction or corruption of information stored on a network connected to the Internet.	• Denial of service attack resulting in degraded services to the public. • E-mail virus resulting in degradation of e-mail services for the agency. • Destruction or compromise of data supporting website functionality.

2.33 Each of the 10 agencies participating in this audit was asked to supply a copy of the risk management documentation for the agency's Internet presence. Table 3 indicates those agencies which ANAO considers have developed, or had their contractors develop, appropriate risk assessments in respect of the three elements of their Internet presence.

Table 3

Internet security risk assessments

Agency	*Internet E-mail*	*Browser Services*	*Agency Web Site*
ABS	✔	✔	✔
ACCC	✔	✔	✗
ACS	✔	✗	✗
AEC	✗ Out of date	✗ Out of date	✔
AFFA	✔	✔	✔
ARPANSA *	✗	✗	✗
ATO	✔	✔	✔
DEWRSB	✔	✔	✔
DHAC	✔	✔	✔
Treasury	✔	✔	✔

* ARPANSA's corporate network is provided through DHAC. The ARPANSA and DHAC websites are hosted by the same provider but ARPANSA also hosts another website, in-house, on the Scinet network. The above information relates only to ARPANSA's Scinet network.

Audit findings

2.34 Table 3 shows that six agencies had conducted and documented a risk assessment addressing all three elements of their Internet presence. Although the AEC provided documentation related to each element, the risk assessments for e-mail and browser access were out of date. The ACCC had not documented a risk assessment for the agency's website, while the ACS had only addressed risks associated with Internet e-mail. ARPANSA had not conducted or documented a risk assessment for any element of the agency's Scinet network.

2.35 ANAO considered two of these sites, ACCC and ACS, to represent a lower level of risk to the agencies as the websites are not connected to the agencies' internal networks. Neither site supports electronic transactions. Each contains information about the agency, its services and publications. The site hosted by ARPANSA was connected to the agency's internal network. The ANAO considers that ARPANSA's decision to host this site should have been preceded by a thorough risk assessment.

Internet security policies

2.36 The PSM presents a clear statement about the need for each agency to develop an information security policy:

> *An agency cannot achieve an appropriate security environment for its information resources until it has followed the steps below.*
>
> - *Develop an information security policy …*
> - *Identify the risk to information resources …*
> - *Treat the identified risks.*[26]

Audit findings

2.37 All agencies participating in this audit provided the ANAO with some form of information security policy, usually referred to as the agency's IT security policy, or in the case of larger agencies managing their Internet presence in-house, an Internet security policy or Gateway security policy.

2.38 The AEC policy was developed and related to a time before AEC's move to an outsourced environment. A revised policy, reflecting the agency's current IT environment, was under development at the time of the audit.

2.39 During preparations for outsourcing the Group 8 IT infrastructure, AFFA played a major role in developing the Group 8 IT security policy, and subsequently adopted that document as the AFFA IT security policy. A difficulty with this approach was that the Group 8 IT security policy was structured to apply to the Group as a whole. It called for each agency in Group 8 to use the high level document to structure an agency specific security policy which would reflect the distinctly different business objectives and organisational contexts of the different agencies. Consistent with this, ANAO recommended that AFFA prepare an agency-specific IT security policy.

2.40 The ATO's Internet security policy documentation was firmly based on the results of a threat and risk assessment. Different elements of the ATO framework such as the security policy, protective security plan and business continuity plan were extensively cross-referenced, illustrating clear links between the identified threats, risk levels, countermeasures, policy objectives and assumptions.

[26] PSM 2000—Part C, Information Security, p. C16.

2.41 DEWRSB adopted a slightly different approach to its security documentation. Rather than base the policy on a whole-of-agency threat and risk assessment, the DEWRSB IT security policy required that each System Manager identify the risks related to a particular system or data holding and then implement measures designed to reduce the risks to acceptable levels.

2.42 DEWRSB has developed and implemented a management system to support the achievement of this security objective. Called the Production Application Checklist (PAC), it provides a comprehensive, well documented audit trail of actions and decisions surrounding the introduction of any new IT system or application, including online applications.

2.43 The PAC encompasses a detailed security strategy, technical specifications and description of service arrangements along with a threat and risk assessment for each major application. Each element of the PAC must be satisfactorily completed, tested where appropriate and endorsed by relevant senior executives prior to any new system or application being deployed into the DEWRSB production environment. The ANAO considered the DEWRSB PAC arrangements to represent an example of better practice in the management of Internet security.

2.44 In the Department of the Treasury, a comprehensive IT security policy is augmented by a document titled "IT security policy—personal responsibilities". This document outlines the responsibilities of individual staff to maintaining a secure IT environment for Treasury. Providing guidance on matters such as passwords, portable computers, e-mail and the responsible use of official information, the document contributes to maintaining a high level of user awareness and to user education.

2.45 DHAC's IT security policy was similar in structure to that of DEWRSB in that System Managers were clearly identified and assigned particular responsibilities. The DHAC policy addressed issues such as change control procedures, the use of access profiles, user identification codes and password policies. In common with many other agencies' policies, the DHAC policy called for the preparation of a security plan, in the case of DHAC for each major system in the IT environment.

2.46 The DHAC IT infrastructure extends to ARPANSA. That is, ARPANSA operates a corporate network delivered through DHAC by DHAC's outsource provider. ARPANSA had adopted the DHAC IT security policy, with minor changes, as the ARPANSA IT security policy. However, ARPANSA maintains a second network supporting scientific research and other business activities. Because this second network is significantly different to the agency's corporate network, the adopted

IT security policy is not directly applicable to it. ANAO recommended that ARPANSA revise its IT security policy to adequately incorporate all elements of its IT environment.

Internet security plans

2.47 As noted above, many security policies require the preparation of one or more security plans. This audit concentrated on security plans pertinent to the Internet presence of the agencies involved.

2.48 The most extensive Internet related security plans were developed by the larger agencies which managed their Internet presence in-house, some with the assistance of contractors or IT infrastructure providers.[27] Typically the Internet security plans contained considerable detail regarding the risk mitigation strategies and technical measures to be adopted by the agency concerned.

Audit findings

2.49 Treasury's Internet Gateway Security Plan represents one element of a wider Treasury Systems Security Plan. Based on the format recommended in ACSI-33, Treasury's plan deals with the firewall and related components of the Internet gateway. Among other things, the plan covers areas such as security administration, logical access control, audit, quality assurance, system integrity, contingency handling, education and training and users' obligations.

2.50 In addition, to the Internet Gateway Security Plan, Treasury's gateway operation was supported by a formal Access Plan, Design Plan, Incident Response Plan and an IT Disaster Recovery Plan. Collectively this documentation represents a detailed set of critical information, management systems and security procedures to support the achievement of Treasury's Internet security policy objectives.

2.51 DEWRSB presented a similarly comprehensive set of planning documents relevant to its Internet gateway. The Gateway Security Plan addressed, among other things, security objectives, threat and risk assessments, physical security controls, communications and logical security controls, backup and quality assurance procedures. The Plan also outlined extensive logging, audit and accountability procedures. In addition DEWRSB had documented an Access Policy, Forensic Plan, Incident Response Plan and a range of procedures addressing change control.

[27] Although an agency may have outsourced provision of its IT infrastructure, its Internet presence may be managed in-house or in partnership with the outsource provider but with a significant in-house component.

2.52 DHAC's Internet security policy is supported by individual system security plans which incorporate an assessment of any significant risks which might apply to a system and are not covered by existing corporate security measures. Specific countermeasures are then identified and included in the system security plan.

2.53 Agencies outsourcing part or all of their Internet presence typically did not produce Internet security plans. There was a clear expectation by agencies that the service provider would have developed its own operational plans having due regard to security matters. Some of the contracts underpinning these arrangements require the service provider to comply with an agency's security policy but the agency is not usually involved in the detailed planning for the delivery of the particular service.[28]

2.54 The DSD certified gateway provider referred to earlier in this report was required, as part of the certification process, to possess adequate security and operational plans. This affords the agencies accessing services from this provider a certain level of confidence in the security outcomes likely to be realised. Other Internet service providers assessed during this audit were not necessarily able to demonstrate a formal security planning framework. This is not to say that the security measures employed by these providers were ineffective or inadequate. Rather, that a formal security plan had not been prepared by the provider, although most had generated a list of standard operating procedures particularly in relation to ensuring system availability and regular data back-ups.

Business continuity planning

2.55 In January 2000, the ANAO released a Better Practice Guide on Business Continuity Management.[29] The Guide highlighted the fact that the continuity of public sector business is a critical issue to be considered by boards, chief executive officers and senior management in the Australian public sector. It noted that many services delivered by government organisations are critical to the economic and social well-being of the Australian society, and observed that a failure to deliver these could have very significant consequences for those concerned.

[28] The issue of contract management is explored later in this report.

[29] Business Continuity Management—Keeping the Wheels in Motion. A Guide to Effective Control. Jan 2000, ANAO.

2.56 Business continuity planning is an integral component of a sound business management system and should form part of any IT security management system, where IT is a critical element of service delivery. A well conceived business continuity plan (BCP) works in conjunction with an agency's risk assessment and security management systems to ensure effective service delivery under the widest range of circumstances.

2.57 A comprehensive BCP addresses circumstances arising from the realisation of any of the risks identified in the risk assessment process. It should identify response strategies along a continuum, from relatively minor business interruptions to a consideration of the worst-case scenario.

2.58 As the deadline for achievement of the *Government Online* agenda draws closer[30] indications are that many more government agency websites will evolve to deliver a greater range of services electronically, and that the Internet delivery mechanisms employed by agencies will increase in complexity. Websites with an enhanced transactional facility also raise the stakes in terms of potential negative impact on an agency from any failure to deliver those services.

2.59 The ANAO examined the BCPs of the 10 agencies involved in this audit. The following Table highlights those agencies that provided the ANAO with a relevant BCP addressing each of their Internet functions.

Table 4

Business Continuity Plans relevant to agency Internet facilities.

Agency	*Internet E-mail*	*Browser Services*	*Agency Web Site*
ABS	✔	✔	✔
ACCC	✔	✔	✖
ACS	✔	✖	✖
AEC	✔	✔	✖
AFFA	✔	✔	✔
ARPANSA *	✖	✖	✖
ATO	✔	✔	✔
DEWRSB	✔	✔	✔
DHAC	✔	✔	✔
Treasury	✔	✔	✔

* ARPANSA's corporate network is provided through DHAC. The ARPANSA and DHAC websites are hosted by the same provider but ARPANSA also hosts another website, in-house, on the Scinet network. The above information relates only to ARPANSA's Scinet network.

[30] See paragraph 1.3.

Audit findings

2.60 Table 4 reveals a similar situation to that presented in Table 3, Risk Assessments. The agencies that had not conducted risk assessments for particular elements of their Internet presence had also not prepared a BCP for those elements. The AEC relied upon the back-up and restoration services provided by its primary IT infrastructure outsourcer for e-mail and web browsing services. The contract between AEC and its external website host lacked references to business continuity practices. However, the ANAO noted that AEC's website hosting arrangements changed during the course of the audit. The agency's primary outsourcer had recently assumed the role of hosting the AEC website and AEC advised that a BCP for the AEC website would be prepared in due course.

2.61 The DSD certified gateway provider used by a number of agencies[31] develops a risk assessment and BCP for each of its clients as one of the contract services. The contingency plans produced by this provider are well structured and give consideration to aspects such as event detection, client notification and service resumption procedures. The contingency plans are tested and regularly reviewed by the provider. These activities are required in order to maintain DSD gateway certification.

2.62 The Australian Customs Service outsources website hosting and Internet browser access (delivered via a series of stand-alone machines rather than directly into Customs' internal network) through a commercial external service provider. ACS did not produce a BCP addressing the agency's web presence or web browsing services. Although the ANAO considered the risks to the ACS via these two services to be minimal, the lack of attention to business continuity management was considered to be a deficiency in ACS's overall management of its Internet presence.

2.63 The ACCC was unable to provide documentation concerning business continuity planning for its website. The ANAO concluded that the ACCC's outsourcer has a selection of standard operating procedures in place that would constitute a BCP if collated and documented. However, in the current environment, ACCC staff do not have recourse to any comprehensive documentation to assure themselves and their executive of the nature of any business continuity service provided by their outsourcer.

[31] See table 1 at paragraph 2.10.

2.64 ARPANSA's corporate network, e-mail, browser and website hosting services, provided through DHAC, were addressed by an appropriate BCP framework. However, the ANAO found ARPANSA's approach to business continuity management for its scientific network to be markedly incomplete.

2.65 The Department of the Treasury had prepared a comprehensive Disaster Recovery Plan encompassing its entire IT environment. The plan outlines detailed procedures for data and systems recovery and clearly indicates the responsibilities, contact details and functions of key staff. The plan also provides guidance on response escalation procedures and includes a schedule for review of the component elements of the plan itself.

2.66 The ABS has developed a set of documentation designed to ensure the smooth recovery of its systems in the event of a disaster. One of the strong features of the ABS IT environment is the availability of a duplicate system, most often used as a test environment, with content tightly synchronised to that of the production environment. Should the ABS experience a significant loss of service delivery capacity, due to either a systems failure or a security incident, a replacement would usually be at hand and so enable the ABS to resume electronic service delivery within a relatively short time frame.

2.67 Duplicate systems also permit the ABS to mirror its web site. Should the site be the victim of a hacker attack and suffer defacement, the duplicate system allows ABS to up-load the last saved version and thereby contain the embarrassment associated with website defacement. This feature was not unique to the ABS. Evidence provided to the ANAO showed that a significant proportion of agency BCPs incorporate some form of website backup and rapid restoration procedure.

Conclusion

2.68 The ANAO noted a strong correlation between the perceived level of risk associated with an agency's Internet presence and the apparent effort devoted to risk assessment and business continuity planning. For example, agencies with an Internet site physically separate from their internal network usually assessed the risks, and consequent impact on business systems should those risks be realised, as low. Such websites contain information designed for public access and provided the sites do not contain valuable databases or files not intended for public access, the risks to the agency are minimal.

2.69 The most obvious risk associated with operating such a website is the risk of defacement. While a website defacement may cause the agency some degree of embarrassment and reduce public access to the site's resources for a short period while the compromised files are replaced, the confidentiality of Commonwealth information is not jeopardised. The majority of audited agencies with low risk websites, had adopted a less formal and less comprehensive approach to risk assessment and business continuity planning.

2.70 On the other hand, agencies supporting more interactive websites wherein users can interrogate databases, lodge applications or official forms, transfer personal information or conduct financial dealings whether these be purchasing a product or paying a license or other fee, must address a higher level of risk. Firstly, risks to the confidentiality, integrity and availability of Commonwealth information assets are greater in an interactive online environment. Secondly, the risks to an agency's business functions or its ability to deliver services via the Internet increase appreciably.

2.71 During this audit the ANAO found that agencies supporting the more sophisticated, interactive methods of electronic service delivery, devoted more resources and embraced a more formal approach to risk assessment, risk management and business continuity planning activities.

2.72 While this approach is generally consistent with the application of a risk management model, the ANAO notes that low risk does not equate with no risk. Agencies that entirely neglect to assess risks and plan to ensure continuity of service to their clients, could not be said to be managing risk effectively.

3. Elements of Internet site management

This chapter discusses some of the more important elements of Internet site management including the security features often associated with static and transactional sites or sites which deal with personal or sensitive information. The chapter also compares security management in an outsourced vs in-house environment.

Security features of static and transactional sites

3.1 Six of the 10 agencies involved in the audit operate one or more static websites. That is, the websites contain publications, brochures and information intended to be publicly accessible. Internet users typically navigate the site to search for and access the publications of interest to them.

3.2 Four of the 10 agencies operate one or more transactional websites. In addition to providing the services of a static site, such transactional websites support user access to password protected areas, enable visitors to the website to purchase goods online or contribute to live discussions or message boards on a site. Transactional sites also permit users to interrogate databases and extract information or to lodge information via an electronic form or a specific piece of software.

3.3 ANAO noted that the four agencies incorporating transactional web content managed their Internet sites, or at least the transactional components of these, using in-house resources.

Audit findings

3.4 ANAO found that, for the most part, the security of transactional sites is well managed. The security policies, plans and management structures surrounding these systems ensure a level of security commensurate with the level of risk associated with the sites. Typically, these sites employ extensive logging and auditing of user access, along with automated intrusion detection systems and active monitoring by agency IT personnel.

3.5 DEWRSB hosts the Business Entry Point (BEP) site which, through the Australian Business Register, allows Australian individuals and businesses to apply online for an Australian Business Number (ABN). Having regard to the sensitivity of databases containing significant quantities of personal and business information, DEWRSB afforded the site due consideration in its risk assessment, physical and logical security measures and in the development of a detailed business continuity plan.

3.6 An ATO website supports the electronic lodgement of Business Activity Statements (BAS). The facility employs Public Key Technology (PKT) to encrypt and therefore ensure the security of these transactions and to authenticate the identity of a user or business lodging a BAS.

3.7 ARPANSA's Internet environment featured a password protected 'members only' section that allowed a user with an account and password to access a particular data base on the agency's network. This data base contained documents that attracted an "in-confidence" security classification, although accessible via the Internet. ANAO found this to be a poor practice given that ARPANSA maintained a more secure network, which was better suited to the storage of classified documents. ARPANSA has informed the ANAO that use of the data base has been suspended until such time as further security measures and a threat and risk analysis have been implemented.

Security features of sites dealing with personal or commercially sensitive information

3.8 When Commonwealth Internet sites are used to transmit personal information or commercially sensitive information, the agencies concerned should have regard to privacy issues and employ appropriate technology to ensure secure transmission of this information. The ATO site assessed during this audit was chosen as an example of an Internet gateway for the transmission of personal and commercially sensitive information between individuals and the ATO. This particular site, the ATO's Electronic Commerce Interface (ECI) site, serves as a gateway for businesses to lodge Business Activity Statements (BAS) electronically.[32] The ECI employs PKT to secure the transactions[33]. PKT uses a form of cryptography that allows two parties to communicate in such a way that a third party is unable to determine the content of the message or alter the message without detection. It is designed to assure confidentiality and integrity of information passed between two parties over the Internet. PKT can also provide authentication of identity and non-repudiation in online transactions.

[32] Paragraph 2.25 also describes some features of the ATO's ECI site.

[33] PKT is sometimes referred to as PKI, Public Key Infrastructure. PKT essentially refers to the technology itself; PKI to an administrative infrastructure, based on a hierarchy of trust involving third parties such as Registration Authorities and Certification Authorities, in which a range of PKTs may be employed.

3.9 The Office of the Federal Privacy Commissioner, in June 2001, released a Consultation Paper on “Privacy Issues in the Use of Public Key Infrastructure for Individuals *and* Possible Guidelines for Handling Privacy Issues in the Use of PKI for Individuals by Commonwealth Agencies”. In that paper, the Privacy Commissioner notes that PKI clearly has the capacity to enhance privacy, but that mis-use of PKI has its own associated privacy risks. Agencies should consider these risks when choosing to use PKI and have regard to the Privacy Commissioner’s Guidelines, if and when these are published.

3.10 The heart of PKI is the use of digital signature certificates. The Commonwealth Government has established the ‘Gatekeeper’ program, administered by NOIE, to provide an assurance framework for PKI use by agencies. The Commonwealth Government requires that any online authentication certificates issued by Commonwealth agencies to business and individuals be compliant with the Gatekeeper framework. In March 2001, the Government announced that digital signature certificates issued by Project Angus[34] members, that conform to the Australian Business Number—Digital Signature Certificate (ABN-DSC) standard, would be accepted by Commonwealth agencies. These certificates are capable of handling information classified to the “In-Confidence” level with limits on financial transactions to be determined by transacting parties. NOIE advises that these certificates will be handled in accordance with the ‘Broad Specification for the ABN-DSC’ issued by NOIE, which is the same manner in which ABN-DSCs issued by other Gatekeeper service providers are handled.

Audit Findings

3.11 Establishment of the Electronic Commerce Interface (ECI) site was well planned and extensively documented, including risk assessments, security policies and plans, along with a disaster recovery and business continuity plan. Physical security of the facility was sound. Site management was tightly controlled with firewalls administered remotely via encrypting modems. The operating system and web servers were generally well configured although DSD identified some vulnerabilities and areas for improvement.

3.12 Through its management of online security arrangements, the ATO demonstrated an appropriate sensitivity to the nature of the data and to the agency’s responsibility to safeguard the privacy of individuals using the facility.

[34] Project Angus is a working group involving four of Australia’s large banks to establish a framework for e-commerce trust and authentication using the international Identrus scheme.

Contract management

3.13 A number of agencies had contracted third parties to host their Internet sites. In some instances the contractual relationship existed directly between the agency and the provider, in others an agency's IT outsourcing partner had, with agency agreement, entered into a contract with a specific Internet site host. On occasion a site host had sub-contracted part or all of the function to yet another party.

3.14 Most agencies' IT security policies explicitly acknowledge that responsibility for information security rests with the Chief Executive Officer of the agency or Secretary of the Department. Responsibility for the day to day delivery of security services is usually delegated to senior staff and often rests with the agency's designated IT Security Adviser[35]. Yet during this audit, few agencies that had outsourced website hosting could demonstrate a reasonable understanding of the nature of the security measures provided by their website hosts, and some agencies were not fully aware of the contractual relationships surrounding their website hosting arrangements.

3.15 Such a situation acts directly against an agency's ability to effectively manage its contracts, monitor the level of service provided by contractors and so assure the Chief Executive Officer or Secretary that appropriate security outcomes are actually achieved.

Audit findings

3.16 Some of the contracts for website hosting services examined during this audit, failed to specify expected service levels or lacked clear performance indicators. This contributes to a reduced ability on the part of agency staff to be appraised of the security measures applicable to their website hosting and so to effectively manage the security outcomes for their agency.

3.17 For example, under the heading of security, one contract simply stated that the contractor is responsible for the integrity of the data held on the agency's website. While it may be appropriate to identify expected outcomes in a contract, without the support of a service level agreement or clear performance indicators, those managing the contract are likely to be less well informed about the nature and quality of services delivered. In this example, there was little indication of how website security would be achieved, nor how data integrity would be monitored and reported

[35] The PSM 2000 requires that each agency appoint an IT security adviser. See Paragraph 4.9, p. A16, PSM 2000.

to the agency. While many agency contract managers appeared to inform themselves of the security arrangements at the commencement of the hosting agreement, primarily in regard to the technical level controls, without regular communication between the parties it is possible that a 'set-and-forget' mentality will be adopted.

3.18 In one case an agency had outsourced its IT infrastructure, as part of the Whole-of-Government IT Infrastructure Consolidation and Outsourcing Initiative, while maintaining an arrangement with a different contractor for the provision of a range of network services in support of a major business function. When the agency decided to establish an Internet site, it chose for the network services contractor to sub-contract for web hosting services.

3.19 The original contract for network services did not include a provision for Internet connectivity. Consequently the contract contained nothing in the way of service level expectations, minimum standards or performance measures in respect of Internet security. During the audit, agency staff claimed to have little knowledge of the nature of any contract between their network services contractor and the sub-contractor. Agency staff relied totally upon the network services contractor to manage the delivery of appropriate Internet security measures for their website. In such circumstances, it is unclear how the agency IT staff might reliably assure themselves or their Chief Executive Officer that appropriate Internet security measures were being realised.

Features of better contracts

3.20 Some contracts examined during this audit demonstrate a number of features that enhance an agency's ability to effectively manage the contractual relationship and gain a reliable appreciation of the services actually being delivered.

3.21 The provision for formal, regular reporting by the contractor to the agency, against a set of agreed performance indicators, is a fundamental tool for the contract manager. Regular reporting mechanisms, once established, can facilitate a full and free flow of information between the parties and serve to afford necessary security assurances to the agency. Problems are more likely to be resolved quickly if they are detected early and a regular reporting regime should be designed to identify any problems or difficulties in the early stages.

3.22 A set of minimum standards for Internet security should be included in any contract for hosting Commonwealth Internet sites. Explicit minimum standards provide clarity to both parties regarding expectations or deliverables and may serve as a framework for performance reporting by the contractor.

3.23 The Commonwealth PSM 2000 contains an explicit reference to the responsibilities of contractors engaged to store, process or originate official information. Contracts should contain appropriate references to the PSM and where necessary to ACSI-33, formally acknowledging those responsibilities. Equally, when a contractor sub-contracts part or all of a service, the PSM calls for the sub-contractor to be bound by the same security provisions as the primary contractor, and for the sub-contract to specify this.[36]

Audit findings

3.24 The better contracts examined during the audit contained provisions for agency staff or their nominees to conduct audits of the security measures employed by the contractors in respect of agency websites. A number of contracts also included a provision for the Auditor-General and the Privacy Commissioner to audit the contractors' security procedures and to involve staff from DSD and ASIO as appropriate.

3.25 Contracts incorporating such provisions empower Commonwealth agencies to actively, reliably and effectively manage their contractual relationships and thereby fulfill the responsibilities imposed by the Commonwealth's information security framework.[37]

3.26 In June 2001 the Auditor-General published a set of Standard Access Clauses for use in Commonwealth contracts. Extracts from the Auditor-General's correspondence to agency heads on the use of these clauses in Commonwealth contracts, together with a copy of the Standard Access Clauses, are at Appendix 2.

In-house site management

3.27 While many agencies have outsourced their Internet site hosting along with the provision for Internet e-mail and browser access, a number of agencies have chosen to manage their Internet presence using in-house resources. Typically, these are medium to large agencies with a business need for a relatively complex Internet gateway, supporting transactional activities or more complex electronic service delivery facilities via the Internet. They are often agencies with substantial data holdings, access to which or at least aggregated information drawn from which, constitutes a major feature of the agency's electronic service delivery activities.

[36] Paragraph 6.22 p F47 and paragraph 2.8 p F10, PSM 2000.

[37] Paragraph 6.19 p F45 PSM 2000.

3.28 Of the agencies participating in this audit, ABS, ATO[38], DEWRSB and Treasury meet the above criteria. One smaller agency, ARPANSA, while outsourcing its web hosting and some other Internet related services through its portfolio parent, also manages an Internet connection, including additional website hosting and a second network for the agency.

3.29 Agencies that chose to manage their own Internet sites, rather than outsource the function, appeared to do so for sound business reasons. While a contractor may be able to provide a similar or even more advanced technical solution, for some agencies the element of direct control of the facilities, at this stage of their development, was a primary consideration. This was particularly so for those agencies engaging in e-commerce and where their websites supported some form of transaction between Internet users and the agency.

3.30 In-house site management enables the agency to develop web-based applications that interact with corporate databases, often stored on mainframe computers[39] or integrate more effectively with other corporate IT systems. From an agency's business perspective, a number of web-based applications require access to corporate database information in 'real time'. These applications can be finely tuned to the specific business needs of the agency and are more readily open to timely modification or enhancement. Provided the agency maintains a sufficient resource of skilled staff, there is a perception that responsiveness is enhanced in an environment where Internet applications are managed in-house.

3.31 For some agencies, privacy issues and the ability to control access to sensitive corporate data were considered drivers for in-house site management. Following risk assessments, some agencies decided that devolving custody and/or management of such data to a third party would introduce an unnecessary and unacceptable risk.

3.32 ANAO concluded that the larger agencies appeared better placed to take advantage of the economies of scale associated with hosting multiple websites in-house. These agencies appeared more able to devote the financial and human resources necessary to ensuring effective service delivery and appropriately managed security arrangements.

[38] While ATO has outsourced its IT infrastructure, the elements of the ATO Internet presence assessed during this audit are essentially managed by ATO staff, in partnership with their infrastructure service provider.

[39] It is neither feasible nor desirable for many of the large corporate databases to be stored on a webserver, or for the mainframe to run software enabling direct connection to the Internet.

3.33 They maintained a group of skilled staff, sometimes supported by specialist contractors, and often ascribed an observable, high corporate priority to the security arrangements surrounding their networks and web sites.

3.34 Each of these agencies had typically engaged in a comprehensive risk assessment exercise, regularly involving the different business lines within an agency. Able to build upon existing management structures, the larger agencies had more readily incorporated Internet security management arrangements into their day-to-day business management practices.

3.35 ARPANSA's experience contrasts to that of the larger agencies managing their Internet connectivity in-house. While functioning to meet the research and business needs of the organisation, the second ARPANSA network was not adequately secured against the risks associated with that network's degree and type of Internet connectivity. Due to the relatively small size of the agency, ARPANSA did not apply the necessary resources to planning for and managing Internet security at a level commensurate with the risks of its Internet presence.

3.36 In contrast to other agencies managing in-house, ARPANSA did not develop a formal Internet security policy framework for its second network, nor did the agency integrate the management of security for this network into the relevant business management structures. At the time of this audit, ARPANSA's interim IT security manager had only recently been appointed and the management of IT security was in a transition phase, awaiting the recruitment of a suitable replacement. The lack of an agreed policy, plan and procedures hindered the temporary IT security manager's ability to effectively manage security arrangements for ARPANSA's second network.

Hosting other parties' websites

3.37 Some agencies not only host their own sites, but also host those of other agencies, often within the same general portfolio area. One particular agency hosts Internet websites for a number of smaller agencies and special interest groups within the general portfolio. At the time of the audit, these websites were hosted on the same physical machines as the agency's own websites. While such an approach has the advantage of affording the smaller agencies the protection of a large and complex Internet gateway, usually at little or no cost, it does have the potential to present a significant security risk to the agency hosting these websites.

3.38 In this particular case, a number of security vulnerabilities were identified in the applications associated with the other sites hosted. A number of the applications on hosted sites presented an application level vulnerability which would permit unauthorised access to sections of the operating system. In that event, the host agency's webservers and the information held on those would be at risk. The agency concerned employed a rigorous system of quality control for material placed on its own websites, but at the time of the audit, did not extend this system to apply to all website material provided by other agencies and groups.

3.39 While it may be appropriate for an agency hosting other sites to expect the authors or owners of applications and data to accept responsibility for certain security measures, it is in the best interests of the hosting agency to assure itself that adding such material to its webservers does not introduce unexpected vulnerabilities into its systems.

Outsourcing Internet site management

3.40 For many agencies the drivers for in-house site management are not relevant, and contracting for Internet site hosting services is an attractive option, particularly for a straight-forward Internet site. Such sites generally represent low-risk sites. Typically, all information on such sites is intended to be available to the public. Although, in order to deliver the service some applications may call upon databases that are not intended for public access, and these databases need to be adequately protected.

3.41 Many smaller agencies have determined that it would be too expensive for them to establish and maintain their own secure Internet gateway and so have engaged contractors to host their website. Contractors offer differing levels of security service and an agency is able to select the security measures it considers appropriate for the protection of Commonwealth information held on its Internet site. Some providers offer webservers that only host government sites, others host a mixture of commercial sites alongside government sites while still others provide the option of a dedicated machine for individual sites. Some providers have sought and obtained Internet Gateway Certification from the Defence Signals Directorate, thereby demonstrating to prospective clients the ability to deliver certain levels of service and security, as verified by an external certifying body.

3.42 In order to make informed decisions about outsourcing their website hosting each agency, regardless of size, should conduct a risk assessment. They should identify and document the agency's security requirements in sufficient detail to enable a contractor to clearly comprehend the expected security outcomes and the agency contract managers and contractors should agree upon and establish a regular monitoring and performance reporting framework.

3.43 In order to afford the agency's CEO an appropriate level of comfort in respect of the efficiency of chosen security measures, a regular and comprehensible flow of performance information is essential. In an environment where an agency has outsourced its website hosting, the provision of such performance information should be a fundamental component of the agency's contract management activities.

Conclusion

3.44 There was a strong parallel between the trends observed in relation to security planning and documentation, and those evident in the degree of active management of the agencies' Internet presence. That is, the smaller agencies with a relatively low risk Internet presence were less likely to document a formal risk management strategy and were less likely to devote significant resources to the day to day management of Internet security, whether their Internet presence was managed in-house or outsourced.

3.45 Larger agencies with higher Internet risk profiles, and whether outsourced or managed in-house, consistently demonstrated a more formal and comprehensive approach to contract management and the delivery of security services.

3.46 Agencies operating higher risk websites demonstrated much greater attention to matters such as intrusion detection, active monitoring of access and site usage, business continuity planning and the regular testing and review of these arrangements.

3.47 As noted in the discussion of planning and documenting Internet security practices, this finding is consistent with the application of a risk management model. ANAO's previous observation applies to the active management of Internet security, in that low risk does not equate with no risk. ANAO concluded that some smaller agencies had adopted a 'set-and-forget' mentality. An effective application of a risk management model would see agencies implementing Internet security control structures commensurate with the level of identified risk.

4. Internet Security Outcomes

This chapter reports general findings of the security testing of selected Commonwealth websites.

Overall Internet site test results

4.1 Staff from the Defence Signals Directorate were appointed under provisions of the *Auditor-General Act 1997* to assist the ANAO in the conduct of this audit. The DSD team performed a detailed technical examination of selected web servers, mail servers and other Internet services in each agency. An element of the technical examination involved assessing sites against a range of publicly known vulnerabilities.

4.2 Where DSD was able to demonstrate a vulnerability, this was brought to the attention of the agency along with advice on how to overcome the vulnerability. As a result, any serious security vulnerabilities identified during this audit were promptly addressed. Often, a security 'patch' or a technical advisory note, specifically designed to fix a particular problem, had been released by the relevant software vendor. In some cases a detailed risk assessment or review of website architecture was called for to ensure a comprehensive application of security controls to all elements of an agency's web presence.

4.3 Six of the agencies were found to manage websites containing significant vulnerabilities, potentially exploitable by a malicious user over the Internet. Two of these were rectified with the application of a security patch, and a third by a change in the access permissions of a particular class of users. The vulnerabilities identified in the remaining three sites arose from the inconsistent application of security controls to all elements of a site. While the rectification of each vulnerability was readily addressed, the agencies were advised to conduct a thorough risk assessment and review the implementation of agency security policy.

4.4 In addition, DSD identified other security issues in all sites. The technical assessments resulted in a total of 97 recommendations to agencies, all of which were accepted by agencies and the majority of which have been implemented. A small number of recommendations encouraged agencies to embark upon a course of action extending over several months. The ANAO considers that agencies have made satisfactory progress in the implementation of such medium-term recommendations.

4.5 The fact that 97 technical recommendations were made does not mean that 97 exploitable vulnerabilities were identified during this audit. Many of these recommendations were aimed at increasing existing security levels, i.e. intended to make a relatively secure installation even more secure and to promote the use of better practice in web server configuration and management.

4.6 The remainder of this chapter outlines a number of general findings from the technical assessment phase of the audit. Specific findings in relation to individual websites are not included, as to have published such information would introduce an unnecessary risk to the security of those, or similarly configured, websites.

Documentation

4.7 Agencies were asked, prior to the commencement of the technical phase of the audit, to provide documentation including security policies and plans, threat and risk assessments (TRA), network diagrams, and a description of their Internet services, assets and connectivity.

4.8 The quantity, quality and currency of the documentation provided varied considerably between agencies. Some agencies failed to provide all requested material, and in some cases the documentation provided did not reflect the current IT environment within the agencies.

4.9 The audit team observed that, in general, agencies that managed their Internet gateway in-house, had developed and maintained superior levels of documentation. Documentation from agencies that had outsourced part or all of their IT environment was often found to contain inconsistencies, or to have gaps in coverage.

Perimeter security

4.10 Perimeter security, for the majority of agencies audited, was appropriate in terms of the high level configuration of the gateway. This includes the effective use of routers and firewalls, or the outsourcing of the entire gateway environment to a provider operating a certified gateway.

4.11 Government policy for Commonwealth agency Internet gateways, as stated in the ACSI-33 and the PSM, is that all classified networks connecting to unclassified networks such as the Internet must use an appropriately evaluated and configured firewall. It was found that a number of agencies whose web sites were located within their Internet gateway were using firewalls other than these.

4.12 Physical security was found to be generally acceptable. In some cases, the Australian Security Intelligence Organisation (ASIO) had certified the facilities housing the web servers, demonstrating that a suitable level of physical security had been achieved. One agency audited demonstrated very poor physical security.

Server configurations

4.13 Agencies were observed to exhibit considerable variation in the security of web server operating systems, with most agencies assessed as either quite good, or quite poor. Investigations showed that those agencies that had built their servers on a well-planned, securely configured operating system base were rewarded with a more secure system, even when as occurred in some cases, other aspects of good security practice were not followed later.

4.14 Many agencies were observed to have servers running unnecessary network services. Such services may represent vulnerabilities in an otherwise secure configuration. In some cases, these services were permitted through to the Internet, due to either poorly configured perimeter security, or a lack of any access control devices between the server and the Internet.

4.15 Patching of system software to reduce susceptibility to known vulnerabilities is an important part of maintaining appropriate security levels. The audit revealed that procedures for monitoring the release of patches and managing their installation were often unreliable, with several agencies operating out-of-date software on critical systems.

Administration

4.16 Password policies, as documented, were found to be appropriate in the majority of cases. However, the implementation was not always as satisfactory. Default passwords were discovered on systems and devices in two agencies, while a third was observed to distribute new passwords over the telephone. This practice raises questions about the quality of any procedure employed to verify the identity of a user.

4.17 Change control procedures were generally found to be good, although in one case it was noted that a major change to the system had been introduced without the knowledge or approval of the agency’s IT Security Manager.

4.18 There was a lack of clarity in the roles and responsibilities of various parties when the management of a web site was contracted out. In two instances the management of an agency's website had been subcontracted by the original contractor. Unless carefully managed, subcontracting can act to increase the distance between agency staff and the third party administering the site. In these two cases, agency staff demonstrated a reduced level of awareness about the security measures surrounding their websites.

4.19 In the case of a third agency, the audit team noted that one organisation was responsible for the administration and security of the web server's operating system while agency staff were responsible for the administration and security of the web server software. Again, without careful management to ensure clear roles and responsibilities for key players, breakdowns in communication are more likely to occur and consequently some required security related tasks are less likely to be performed in a timely manner.

4.20 The audit team formed the opinion that when websites were hosted and managed internally, the level of coordination and communication between relevant groups was substantially better than when the sites' management was contracted out. Co-ordination issues arising in outsourced situations did not appear to be insurmountable. Adequate co-ordination and security can be achieved if service level agreements covering the requirements are well-defined in outsourcing contracts, and agency staff managing the contract are resourced and trained appropriately.

Intrusion detection

4.21 The majority of agencies audited do not currently implement intrusion detection systems (IDS). Two agencies participating in this audit did operate an IDS and the audit team found these to be generally well-managed. A similar observation was made in relation to the DSD certified gateway provider. No major incidents had been detected by these systems at the time of the audit. Notwithstanding, ANAO considers a well-configured IDS is a strong addition to the overall security of an Internet gateway.

4.22 The use of intrusion detection systems (IDS) is not mandated by Commonwealth policy[40]. However, the additional level of security these

[40] ACSI-33 recommends that intrusion detection capabilities should be installed on all critical gateway hosts and network segments handling security classified material. See ACSI-33, Handbooks 1 and 13.

systems can provide is particularly appropriate for complex, critical or highly sensitive systems where the capability to respond quickly to an incident is important.

Virus prevention and content filtering

4.23 Nine of the 10 agencies involved in the audit demonstrated a sound approach to managing the risk of computer viruses entering their networks. Commercial anti-virus software is readily available and relatively easily employed at many points in the e-mail communications chain.

4.24 Typically, agencies employed virus scanning software to search for known viruses on all incoming e-mail, at the mail server. A second line of protection was often established by installing anti-virus software on each workstation or desktop computer. The anti-virus programs would be configured to run when the desktop computer is switched on and whenever a disk is inserted into the desktop machine.

4.25 Desktop installations of anti-virus software were usually supported by an automatic facility to ensure the latest version of virus recognition files is rapidly and effectively deployed to all workstations on the network. A small number of agencies was found not to be maintaining up-to-date virus signature files. Consequently in those circumstances, the introduction of new or fairly recent viruses would be unlikely to be detected.

4.26 Those agencies that maintain or contract the provision of a secure Internet gateway may also run a third level of virus protection on an external mail server. By using a different software application in each location, i.e. anti-virus software from three different vendors, the breadth of coverage is extended beyond that afforded by use of a single anti-virus product.

4.27 One agency employed anti-virus software at the desktop level, but in such a way that files imported from the Internet would not automatically be scanned for viruses. The network’s architecture and usage patterns - users could and regularly did disable the anti-virus software on their machines - represented obstacles to effective virus protection in that agency. A number of recommendations were made to the agency concerned and these are being acted upon.

4.28 One agency regularly conducted content filtering on all incoming and outgoing e-mail in order to monitor any unauthorised release of corporate information. Other agencies employed content filtering at particular times of the year i.e. when activity was expected to be at a peak or in the lead up to a potentially sensitive publication or announcement.

Auditing

4.29 Most agencies had implemented acceptable procedures for the logging of data, with appropriate data on access and usage being collected and stored. However, the review of these logs to identify potential security breaches was, in general, poorly undertaken. Failure to review logs was often acknowledged by agencies. Most often, relevant staff claimed a lack of time to perform the task, even though a large majority of agency security policies called for logs to be reviewed.

4.30 In a low risk environment, this situation may be justifiable. However, where agency websites support greater functionality or facilitate transactions involving the transfer of sensitive information, appropriate attention to monitoring Internet traffic and regularly reviewing access logs should be ascribed a higher priority. Staff managing the transactional sites assessed in this audit did undertake regular reviews of access and other logs. The audit team offered a number of recommendations designed to improve the efficiency of such reviews, and these recommendations were appreciated by the agencies concerned.

4.31 In some situations, where the Internet gateway environment was contracted out to an external service provider, the provider performed regular auditing of logs, though procedures for advising agencies of the results of these regular reviews were not well defined. In one case the service provider had made the logs publicly available on the Internet, a security issue in itself, yet agency staff were unaware of this.

Websites

4.32 Agency websites varied widely in content and complexity, with some sites being almost entirely static, while others made substantial use of various active coding techniques to provide a more interactive experience for users. Consistent with expectations, site testing revealed that, overall, the static sites presented fewer vulnerabilities than sites containing active content.

4.33 ANAO assessed the development of web applications as generally poor, from a security perspective. There were few indications of secure programming techniques integrated into the development process, the lack of which resulted in a substantial number of vulnerabilities identified during the audit process. The most common issues were with basic active content applications such as feedback and subscription forms, in which user input was not checked to ensure appropriate content. A failure to check user input may result in the introduction of serious vulnerabilities, leading to possible compromise of the web server.

4.34 Some agencies, notably Treasury and DEWRSB, had developed coding standards which incorporated security objectives. The audit team observed that the security level of the web pages produced by these agencies was generally higher than the average, particularly where web page code was formally reviewed for compliance to the standards prior to publication.

Conclusion

4.35 ANAO considered the security levels across the audited agencies to vary widely in quality, from very good to poor. Even the most secure agencies were found to have one potential vulnerability or one procedure which could be described as less than ideal security practice. However, the audit team recognised that, given the complexity of even a relatively simple Internet gateway, it would be unusual not to find any vulnerability.

4.36 Characteristics shared by the better performing agencies were:

- comprehensive knowledge of their systems;
- clearly defined responsibilities;
- an active approach to maintaining security;
- the ability to respond quickly to issues as they arise; and
- adequate staffing levels.

4.37 ANAO noted that participation in this audit appears to have heightened IT staff awareness and improved the quality of website security in involved agencies. The audit has also demonstrated the benefit of regular third party audits or reviews of an agency's website security management. This view is supported by the observation that a number of the agencies have requested that their websites be audited again, at some point in the future. Additionally, as knowledge of the audit spread through the community of IT security managers, DSD and ANAO received inquiries from several agencies, not directly involved in this audit, about the possibility of having their sites audited. Such activity indicates that the security of Internet gateways is regarded by staff within many agencies as a high priority, particularly as the deadline approaches for all appropriate government services to be available online.

Canberra ACT
20 September 2001

Ian McPhee
Acting Auditor-General

Appendices

Appendix 1

Commonwealth Guidance Material on Internet Security

Key government policy and guidance material in terms of Internet security requirements include:

- the *Commonwealth Protective Security Manual 2000* (PSM) maintained by the Protective Security Coordination Centre;
- the *Australian Communications-Electronic Security Instructions–33* (ACSI-33) maintained by the Defence Signals Directorate;
- the *Gateway Certification Guide, version 2.1*, maintained by the Defence Signals Directorate;
- a *Guide to Minimum Website Standards* maintained by the National Office for the Information Economy (NOIE); and
- The Commonwealth *Privacy Act 1988.*

Protective Security Manual

The PSM is the Commonwealth's top-level framework for physical, information and personnel security matters. In his Foreword to the October 2000 release of the PSM, the Attorney-General describes the purpose and intent of the Manual.

> *The* Commonwealth Protective Security Manual *sets out the policies, practices and procedures that provide a protective security environment that is not only fundamental to good business and management practice, but essential for good government. It also lays down the procedures designed to ensure that departments and agencies approach protective security measures in a way that is consistent across government. … The introduction of new work practices such as information technology, contracting, outsourcing and home-based work have all brought significant efficiencies to the business of government, but have also introduced different risks and vulnerabilities that need to be carefully managed. This Manual provides guidance to government departments and agencies for managing those risks.*

Part B of the PSM, Guidelines on Managing Security Risk, addresses the general policy context and outlines a methodology consistent with other government publications on risk management in the APS and the Australian/New Zealand standard on Risk Management (AS/NZS 4360:1999). It also discusses the various roles and responsibilities for security risk management and defines the terms used in the framework. A six-step model is employed to illustrate the key stages of a security risk management process. The section concludes with a set of minimum standards viz:

- the Government expects that each of its agencies will prepare a security plan using risk management principles;
- minimum standards, whether imposed by legislation or government policy, must form part of every agency's security plan;
- each agency must establish and maintain a security environment appropriate to its functions and responsibilities;
- the risk environment must be monitored continuously, the security plan must be evaluated to ensure that the treatments and strategies are effective and cost-efficient.

Part C of the PSM specifically addresses Information Security, highlighting the need to protect the confidentiality, integrity and availability of all Commonwealth information assets. The security of IT systems as well as the information these systems store and transmit is also addressed. In an environment where a significant proportion of IT infrastructure has been outsourced by agencies, it is noteworthy that the PSM places an obligation on agencies to ensure that all contractors who acquire or access Commonwealth information in the course of fulfilling the contract, meet the minimum standards detailed in the PSM.

This section of PSM calls on agencies to develop an Information Security Policy and apply the results of a risk assessment process to formulate an Information Security Plan. It highlights the importance of ensuring appropriate logical access controls, IT system audit trails, protection against virus or other damaging computer code and business continuity planning.

For matters relating to IT security the PSM directs agencies to the Defence Signals Directorate publication, ACSI-33.

Australian Communications-Electronic Security Instructions–33

By Government directive in October 1986, the Defence Signals Directorate was designated as the national computer and communications security authority, and ascribed particular roles in relation to providing advice and assistance to Commonwealth departments and agencies.

DSD has developed a number of Security Instructions, including *ACSI-33 : Security Guidelines for Australian Government IT Systems*, version 1.0, published December 2000. ACSI-33 uses terminology consistent with the PSM and has been written to provide practical guidance to agencies wishing to protect their information systems.

ACSI-33 consists of a number of ‘handbooks’ covering issues such as risk management, network security, web security and minimum standards for the storage, processing and transmission of information classified up to and including the PROTECTED level.

Written to be consistent with the PSM as well as AS/NZS 4360:1999 and AS/NZS 4444:1999 (Information Security Management), ACSI-33 endeavors to categorise security countermeasures into identified risk levels, defined as ‘grades’. These grades may then be used as a tool to assist in identifying appropriate security control measures commensurate with identified risks.

Gateway Certification Guide

DSD offers a Gateway Certification service, which provides an independent assessment that an agency’s Internet gateway has been configured and managed appropriately and that suitable safeguards have been implemented and are operating effectively. The *Gateway Certification Guide* alerts agencies seeking DSD certification to the requirements they must fulfill. The current version of the Guide, version 2.1 published February 2001, also provides suggestions for secure gateway design and management.

As is the case with other Commonwealth guidance material relevant to Internet security matters, the *Gateway Certification Guide* stresses the importance of conducting a security risk assessment as the first step. It identifies minimum standards in relation to an agency’s gateway policy, design and management.

Guide to Minimum Website Standards

The National Office for the Information Economy (NOIE) is the Commonwealth’s lead agency for online issues and coordinates the *Government Online Strategy*. In March 2001 NOIE released its *Guide to Minimum Website Standards* dealing with, among other things, authentication, privacy and security.

NOIE has a clear role in promoting a range of Government Online Security Measures recently announced by Government. In March 2000 the Commonwealth Government reiterated an existing mandate for agencies to comply with the PSM, ACSI-33 and the *Privacy Act 1988*.

In November 2000 the Government introduced additional online security measures including:

- a more active role for NOIE as a coordination point for online security issues;
- improved incident reporting requirements;
- arrangements to facilitate external certification and auditing of agency online security;
- a requirement that any non-government service providers or intermediaries involved in Commonwealth online service delivery comply with standards such as PSM and ACSI-33 and/or participate in an external certification process.

As part of the *Government Online* reporting arrangements, departmental Secretaries and agency CEOs will be expected to report that they have been able to warrant, or not, the compliance of their portfolio online assets with online security standards such as PSM and ACSI-33.

Privacy

All departments and agencies are bound by the provisions of the *Privacy Act 1988*. The Privacy Commission has also issued privacy standards in the *Guidelines for Federal and ACT Government World Wide Websites*. There are four guidelines dealing with:

- openness;
- collection of personal information via a website;
- security; and
- publishing personal information on a website.

The Commonwealth Government expected agencies to have implemented these guidelines by 1 June 2000. The Office of the Federal Privacy Commissioner released the results of a *Privacy Compliance Audit: Commonwealth Government Websites 2001*, in August 2001, in which it was revealed that 31 per cent of Commonwealth Government websites did not display a privacy statement.

Appendix 2

Standard Access Clauses

Extracts from a covering letter from the Auditor-General to agency heads in June 2001.

June 2001

[Agency Heads]

I wrote to all agency heads in September 1997 regarding the use of model access clauses for use in Commonwealth government contracts. These clauses were designed to provide access by both agencies and the Australian National Audit Office (ANAO) to records, information and assets associated with contractors' responsibilities for the delivery of services and/or equipment. The model access clauses attached to that letter were developed by the ANAO in consultation with its legal advisers and the then Department of Finance.

Since that time, the Joint Committee of Public Accounts and Audit, in its Report 368, *Review of Audit Report No.34 1997-98 New Submarine Project—Department of Defence*, recommended, among other things, that:

> *… the Minister for Finance make legislative provision, either through amendment of the Auditor-General Act or the Finance Minister's Orders, to enable the Auditor-General to access the premises of a contractor for the purpose of inspecting and copying documentation and records directly related to a Commonwealth contract, and to inspect any Commonwealth assets held on the premises of the contractor, where such access is, in the opinion of the Auditor-General, required to assist in the performance of an Auditor-General function.*

In response, the Government, in part, stated:

> *The Government supports Commonwealth bodies including appropriate clauses in contracts as the best and most cost effective mechanism to facilitate access by the ANAO to a contractor's premises in appropriate circumstances.*

The Government response also made a commitment to amend the *Commonwealth Procurement Guidelines* to:

> *…emphasise the importance of agencies ensuring they are able to satisfy all relevant accountability obligations, including ANAO access to records and premises. Once the Guidelines have been revised, the Minister for Finance and Administration will write to all Ministers to draw attention to the changes in the Guidelines.*

The Minister for Finance and Administration has now approved revised standard access clauses developed in consultation with the ANAO. A copy of the new clauses is attached for your information. The ANAO considers their use to be particularly important in large contracts for services and/or facilities, such as outsourcing contracts. They would not normally be necessary for 'products' or 'commodity type' services procured in the normal course of business. It is expected that the need for ANAO access would be the exception rather than the rule, particularly if the agency has a robust control environment including sound monitoring and review of private sector involvement.

The Department of Finance and Administration has placed the revised access clauses on its CTC Toolkit (available through its website—www.finance.gov.au) and the ANAO has also placed the revised clauses on its web address <www.anao.gov.au>.

The ANAO would be pleased to discuss this matter with you or your officers if this would be of assistance. The ANAO contact officer in the first instance is Mr Russell Coleman, Executive Director, Corporate Management Branch, tel: (02) 6203 7640 or email: <russell.coleman@anao.gov.au>.

Yours sincerely

Barrett

P J Barrett
Auditor-General

Standard Access Clauses

INFORMATION MANAGEMENT AND ACCESS

AUDIT AND ACCESS REQUIREMENTS

1. Audits under **clause 2** may be conducted of:

   (a) the Contractor's practices and procedures as they relate to the Contract, including security procedures;

   (b) the manner in which the Contractor performs its obligations under the Contract;

   (c) the compliance of the Contractor's invoices and reports with its obligations under the Contract;

   (d) the Contractor's compliance with all its obligations under the Contract;

   (e) the Contractor's compliance with its confidentiality, privacy, security and Commonwealth policy obligations under the Contract; and

   (f) any other matters determined by ***[Agency]*** to be relevant to the performance of the Contractor's obligations under the Contract.

2. AUDITS

2.1 The Contractor must participate in audits of the Contract at the frequency and in relation to the matters specified by ***[Agency]***, (including on an ad hoc basis if requested by ***[Agency]*)**, for the purpose of ensuring that the Contract is being properly performed and administered. ***[Agency]*** may appoint an independent person to assist in the audits. Audits may consider all aspects of the Contractor's performance including but not limited to any performance indicators, benchmarks or targets.

2.2 The Contractor must participate promptly and cooperatively in any audits conducted by ***[Agency]*** or its nominee.

2.3 Except for those circumstances in which notice is not practicable or appropriate (eg. caused by a regulatory request with shorter notice or investigation of theft or breach of contract), and without limiting any other right, recourse or remedy of ***[Agency],*** must give the Contractor reasonable notice of an audit and where reasonably practicable an indication of which documents and/or class of documents the auditor may require.

2.4 Subject to any express provisions in the Contract to the contrary each party must bear its own costs of any audits.

2.5 Subject to **clauses 2.6** and **3.6**, the requirement for, and participation in, audits does not in any way reduce the Contractor's responsibility to perform its obligations in accordance with the Contract.

2.6 ***[Agency]*** must use reasonable endeavours to ensure that audits performed pursuant to clause 2.1 do not unreasonably delay or disrupt in any material respect the Contractor's performance of its obligations under the Contract.

2.7 [Any amendments to the Contract resulting from audits must be effected by agreement in writing between the parties in accordance with the Contract amendment provisions of the Contract.]

2.8 The Contractor must promptly take, at no additional cost to ***[Agency]***, corrective action to rectify any error, non-compliance or inaccuracy identified in any audit in the way the Contractor has under the Contract:

(a) supplied any goods or services; or

(b) calculated fees, or any other amounts or charges billed to ***[Agency].***

3. ACCESS TO THE CONTRACTOR'S PREMISES AND RECORDS.

3.1 For the purposes of **clause 2** and this **clause 3** , the Contractor must, and must ensure that its subcontractors grant ***[Agency]*** and its nominees or the Auditor-General access as required by ***[Agency],*** to the Contractor's premises and data, records, accounts and other financial material or material (including ***[Agency]*** property) relevant to the performance of the Contract, however and wherever stored or located, under the Contractor's or its subcontractors' custody, possession or control for inspection and / or copying.

3.2 In the case of documents or records stored on a medium other than in writing, the Contractor must make available on request at no additional cost to ***[Agency]*** such reasonable facilities as may be necessary to enable a legible reproduction to be created.

3.3 Subject to **clause 2.3** and without limiting any other provision of the Contract, the Commonwealth Auditor-General or a delegate of the Auditor-General or the Privacy Commissioner or a delegate of the Privacy Commissioner, for the purpose of performing the Auditor-General's or Privacy Commissioner's statutory functions and/or powers respectively, may, at reasonable times:

(a) access the premises of the Contractor;

(b) require the provision by the Contractor, its employees, agents or subcontractors, of records and other information which are related to the Contract; and

(c) access, inspect and copy documentation and records or any other matter relevant to the Contractor's obligations or performance of the Contract, however stored, in the custody or under the control of the Contractor, its employees, agents or subcontractors.

3.4 The Contractor must ensure that any subcontract entered into for the purpose of the Contract contains an equivalent clause granting the rights specified in this **clause 3** and **clause 1** with respect to the subcontractor's premises, data, records, accounts, financial material and information and those of its employees, agents or subcontractors.

3.5 This **clause 3** applies for the term of the Contract and for a period of 7 years from the date of its expiration or termination.

3.6 In the exercise of the general rights granted by **clause 3, *[Agency]*** must use reasonable endeavours not to unreasonably interfere with the Contractor's performance under the Contract in any material respect.

3.7 If in exercising the rights granted under clause 1, clause 2 or clause 3 the ***[Agency]*** unreasonably interferes with the Contractor's performance of its obligations under the Contract in a material respect and that interference substantially delays the Contractor in performing its obligations it may request an extension of time to perform its obligations.

3.8 The ***[Agency]*** must not unreasonably refuse a request pursuant to clause 3.7 where the Contractor substantiates the request ,within a reasonable time, to the satisfaction of the ***[Agency],*** provided that:

(a) the Contractor advised the ***[Agency]*** of the delay with *14* days of the exercise of the rights and the delay occurring;

(b) the delay could not have been reasonably contemplated or allowed for by the Contractor before entering the Contract; and

(c) the Contractor has taken or takes all reasonable steps to minimise any delay.

3.9 In no circumstances shall any extension of time pursuant to clause 3 exceed the amount of any delay directly arising from the exercise of the rights.

3.10 In no circumstances shall the Contractor be entitled to any delay costs or other costs or expenses of whatever nature relating in any way to the exercise of any rights under clause 1, clause 2 or clause 3 other than to the extent expressly provided for under clause 2.4.

3.11 Without limiting any of its other obligations under the Contract the Contractor must, at its cost, ensure that it keeps full and complete records in accordance with all applicable Australian Accounting Standards and that data, information and records relating to the Contract or its performance are maintained in such a form and manner as to facilitate access and inspection under clause 1, clause 2 or clause 3.

3.12 If, recognising the obligation in clause 3.11 and the rights under clause 1, clause 2 and clause 3, the Contractor reasonably believes that the exercise of the rights granted under clause 1, clause 2 or clause 3 will cause the Contractor to incur direct expenses which, having regard to the value of the Contract, are substantial and materially exceed those which it would otherwise have to incur in meeting its obligations under clause 3.11 ('excessive direct expenses'), it may give reasonable notice of the exercise of those rights notify the ***[Agency]***. If the Contractor substantiates that its direct expenses in complying with the exercise of the rights in such circumstances are excessive the ***[Agency]*** and the Contractor shall negotiate an appropriate reimbursement, but in no circumstances shall any reimbursement be greater than the direct expenses incurred.

3.13 Nothing in the Contract reduces, limits or restricts in any way any function, power, right or entitlement of the Commonwealth Auditor-General or a delegate of the Auditor-General or the Privacy Commissioner or a delegate of the Privacy Commissioner. The rights of the Commonwealth under the Contract are in addition to any other power, right or entitlement of the Commonwealth Auditor-General or a delegate of the Auditor-General or the Privacy Commissioner or a delegate of the Privacy Commissioner.

TENDER CLAUSE (draft clause)

4. Australian National Audit Office

4.1 The attention of Tenderers is drawn to the *Auditor-General Act 1997* (Cth), which provides the Auditor-General or an authorised person with a right to have, at all reasonable times, access to information, documents and records.

4.2 In addition to the Auditor-General's powers under the *Auditor-General Act 1997* (Cth), if the Tenderer is chosen to enter into a contract, the Tenderer will be required to provide the Auditor-General or an authorised person, access to information, documents, records and ***[Agency]*** assets, including those on the Tenderer's premises. This will be required at reasonable times on giving reasonable notice for the purpose of carrying out the Auditor-General's functions and will be restricted to information and assets which are in the custody or control of the Tenderer, its employees, agents or subcontractors, and which are related to the Contract. Such access will apply for the term of the Contract and for a period of 7 years from the date of expiration or termination.

4.3 Tenderers should obtain, and will be deemed to have obtained, their own advice on the impact of the *Auditor-General Act 1997 (Cth)* on their participation in the Tender.

Index

Series Titles

Titles published during the financial year 2001–02

Audit Report No.12 Financial Control and Administration Audit
Selection, Implementation and Management of Financial Management Information Systems in Commonwealth Agencies

Audit Report No.11 Performance Audit
Administration of the Federation Fund Programme

Audit Report No.10 Assurance and Control Assessment Audit
Management of Bank Accounts by Agencies

Audit Report No.9 Performance Audit
Learning for Skills and Knowledge—Customer Service Officers
Centrelink

Audit Report No.8 Assurance and Control Assessment Audit
Disposal of Infrastructure, Plant and Equipment

Audit Report No.7 Audit Activity Report
Audit Activity Report: January to June 2001
Summary of Outcomes

Audit Report No.6 Performance Audit
Commonwealth Fisheries Management: Follow-up Audit
Australian Fisheries Management Authority

Audit Report No.5 Performance Audit
Parliamentarians' Entitlements: 1999–2000

Audit Report No.4 Performance Audit
Commonwealth Estate Property Sales
Department of Finance and Administration

Audit Report No.3 Performance Audit
The Australian Taxation Office's Administration of Taxation Rulings
Australian Taxation Office

Audit Report No.2 Performance Audit
Examination of Allegations Relating to Sales Tax Fraud
Australian Taxation Office

Audit Report No.1 Financial Statement Audit
Control active contentStructures as part of the Audits of the Financial Statements of Major Commonwealth Entities for the Year Ended 30 June 2001

Better Practice Guides

Rehabilitation: Managing Return to Work	Jun 2001
Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Contract Management	Feb 2001
AMODEL Illustrative Financial Statements 2001	May 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.47 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices	Jun 1999
Managing Parliamentary Workflow	Jun 1999
Cash Management	Mar 1999
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	Jul 1998
Life-cycle Costing (in Audit Report No.43 1997–98)	May 1998
Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997
Audit Committees	Jul 1997
Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies)	Jun 1997
Administration of Grants	May 1997
Management of Corporate Sponsorship	Apr 1997

Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Performance Information Principles	Nov 1996
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996