Cyber Attacks: Securing Agencies' ICT Systems

Introduction

1. Governments, businesses and individuals increasingly rely on information and communications technology (ICT) in their day-to-day activities, with rapid advances continuing to be made in how people and organisations communicate, interact and transact business through ICT and the Internet. In the government sector, ICT is used to deliver services, store and process information, and enable communications, with a consequent need to protect the privacy, security and integrity of information maintained on government systems.

2. Cyber crime is an international problem, and it is estimated that in 2012, 5.4 million Australians fell victim to such crimes, with an estimated cost to the economy of $1.65 billion.[1,2] In the government sector, the Australian Signals Directorate (ASD)[3] has estimated that between January and December 2012, there were over 1790 security incidents against Australian Government agencies. Of these, 685 were considered serious enough to warrant a Cyber Security Operations Centre response.[4]

3. The protection of Australian Government systems and information from unauthorised access and use is a key responsibility of agencies, having regard to their business operations and specific risks. In the context of a national government, those risks can range from threats to national security through to the disclosure of sensitive personal information. Unauthorised access through electronic means, also known as cyber intrusions, can result from the actions of outside individuals or organisations. Individuals operating from within government may also misuse information which they are authorised to access, or may inappropriately access and use government information holdings.[5]

4. For some years, the Australian Government has established both an overarching protective security policy framework, and promulgated specific ICT risk mitigation strategies and related controls, to inform the ICT security posture[6] of agencies. In 2013, the Government mandated elements of the framework, in response to the rapid escalation, intensity and sophistication of cyber crime and other cyber security threats.

Mitigation strategies

5. The Attorney-General's Department (AGD) is responsible for administering the Australian Government's protective security policy, which has as its objective to promote the most effective and efficient ways to secure the continued delivery of Government business. AGD's *Protective Security Policy Framework* (PSPF)[7] outlines the core requirements for the effective use of protective security as a business enabler. To facilitate government working confidently and securely, the PSPF assists agencies to: identify their levels of security risk tolerance; develop an

appropriate security culture; and achieve the mandatory protective security requirements expected by the Government.

6. The PSPF is supported by the *Australian Government Information Security Manual* (ISM)[8], which is released by ASD, and is the standard governing the security of government ICT systems.

7. In 2010, ASD developed a list of 35 strategies to assist Australian Government entities achieve the desired level of control over their systems and mitigate the risk of cyber intrusions. ASD has advised that if fully implemented, the top four mitigation strategies would prevent at least 85 per cent of the targeted cyber intrusions to an agency's ICT systems. This list of strategies is revised annually based on the most recent analysis of incidents.

8. The current top four mitigation strategies are:

- application whitelisting: designed to protect against unauthorised and malicious programs executing on a computer. This strategy aims to ensure that only specifically selected programs can be executed[9];
- patching applications: applying patches to applications and devices to ensure the security of systems[10];
- patching operating systems: deploying critical security patching to operating systems to mitigate extreme risk vulnerabilities; and
- minimising administrative privileges: restricting administrative privileges provides an environment that is more stable, predictable, and easier to administer and support as fewer users can make changes to their operating environment.[11,12]

9. An amendment to the PSPF issued in April 2013, had the effect of: mandating the top four mitigation strategies with immediate effect; and setting a target date of July 2014 for full implementation of the top four strategies. Effective implementation of the mandated strategies assists agencies in achieving control over their ICT systems, providing a higher level of assurance that systems will continue to support the day-to-day business services of the agency.

Selected agencies in this audit

10. Seven agencies were selected by the ANAO to be included in this performance audit:

- Australian Bureau of Statistics (ABS);
- Australian Customs and Border Protection Service (Customs);
- Australian Financial Security Authority (AFSA);
- Australian Taxation Office (ATO);
- Department of Foreign Affairs and Trade (DFAT);
- Department of Human Services (DHS); and
- IP Australia.

11. These agencies were selected based on the character and sensitivity of the information primarily managed by the agency, as summarised in Table S.1.

Table S.1: Key information collected, stored and used by the selected agencies

Australian Government agency	Economic information	Policy and regulatory information	National security information	Program and service delivery	Personal information
Australian Bureau of Statistics	✓				✓
Australian Customs and Border Protection Service			✓	✓	✓
Australian Financial Security Authority	✓	✓			✓
Australian Taxation Office	✓	✓		✓	✓
Department of Foreign Affairs and Trade	✓	✓	✓	✓	✓
Department of Human Services				✓	✓
IP Australia		✓		✓	

Source: ANAO analysis.

Audit objectives, criteria and scope

12. The audit objective was to assess selected agencies' compliance with the four mandatory ICT security strategies and related controls in the *Australian Government Information Security Manual* (ISM). The audit also considered the overall ICT security posture of the selected agencies, based on their implementation of the four mandated mitigation strategies and IT general controls.

13. The ANAO examined agency-level implementation of the 'Top Four' mitigation strategies and related controls mandated in the ISM. In addition, the audit assessed whether the selected agencies had accurately stated their compliance against the ISM controls in their self-assessment reports to the Attorney-General's Department, against the protective security governance guidelines on compliance reporting.[13]

14. The audit also considered the selected agencies' overall ICT security posture, having regard to agencies' implementation of IT general controls[14] and the top four mitigation strategies and related controls. The audit did not consider the PSPF mandatory requirements relating to physical security. A recent ANAO performance audit examined the application of physical security requirements by three Australian Government agencies.[15]

15. In this audit, the ANAO departed from its usual practice of identifying agencies on individual issues due to the risk of disclosing sensitive information about agency ICT systems. In addition, security weaknesses are only addressed at an aggregate level. However, a summary assessment of each agency's performance against the audit objective is provided in Figure S.1.

16. The audit is part of a program of cross-agency performance audits which have examined processes supporting the delivery of services by Government agencies. Since 2000 the ANAO has undertaken 12 cross-agency audits on protective security arrangements. In each of these audit reports the ANAO has encouraged all Government agencies to assess the benefits of the recommendations in light of their own circumstances and practices.

Overall conclusion

17. Modern information and communications technology (ICT) and the Internet are increasingly relied upon by Australian Government agencies as business enablers, to the mutual benefit of government and the community. Benefits include improved access to government services and more cost-effective administration.

18. In this context, the protection of ICT systems and information is a key responsibility of government agencies, and

includes: the prevention of unauthorised access by outsiders seeking to exploit the Internet; and by insiders seeking to misuse their trusted status. Unauthorised access and misuse of government information is an international issue which can affect, amongst other things, national security, the economy, personal privacy, and the integrity of data holdings. The Australian Government has established a protective security framework and identified ICT-specific risk mitigation strategies and related controls which provide a basis for agencies' management of risks to their ICT systems and information. Four key mitigation strategies—intended to control access to ICT systems and apply timely security upgrades—were mandated by the Australian Government in January 2013, and agencies are expected to achieve full compliance with those strategies by July 2014.

19. The agencies subject to audit had established internal information security frameworks, implemented controls designed to safeguard the enterprise ICT environment from external cyber attack, and had stipulated change management processes to authorise the implementation of security patches for applications and operating systems. While these arrangements contributed to the protection of agency information, the selected agencies had not yet achieved full compliance with the top four mitigation strategies mandated by the Australian Government in 2013; a requirement reflecting heightened government expectations in response to the risk of cyber attack. Further, none of the selected agencies are expected to achieve full compliance by the Government's target date of mid–2014, notwithstanding their advice regarding further initiatives which, when implemented, would strengthen ICT security controls and protection against cyber attacks.

20. Based on their stage of implementation of the top four mitigation strategies and IT general controls, the selected agencies' overall ICT security posture was assessed as providing a reasonable level of protection from breaches and disclosures of information from internal sources, with vulnerabilities remaining against attacks from external sources to agency ICT systems. In essence, agency processes and practices have not been sufficiently responsive to the ever-present and ever-changing risks that government systems are exposed to.

21. In the context of working towards compliance with the mandated requirements, it is important that agencies develop a timetable and process to guide implementation in the following key areas:

- deploy the top four mandated ISM controls across the entire ICT environment, to comply fully with Australian Government requirements;
- adhere to a security patch management strategy and deploy security patches in a timely manner, commensurate with assessed risk and using the Australian Signals Directorate's deployment timeframes for vulnerability and patch risk rating;
- restrict privileged user access accounts based on the level of sensitivity of the information; and strengthen access controls to capture and monitor the audit logs for unauthorised access to privileged accounts, and inappropriate activities by privileged users; and
- promote security awareness and accountability within the agency, recognising that security is a shared responsibility.

22. The growth in cyber attacks indicates that an agency's ICT security posture—in essence how well the agency is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats—is increasingly a matter for senior management attention, including agencies' boards of management. Periodic assessment and review of an agency's overall ICT security posture by the agency security executive can provide additional assurance on an agency's resilience to cyber attacks.

23. The ANAO has made three recommendations aimed at improving the selected agencies' approaches to the protection and security of information which they manage. The recommendations are likely to have applicability to other Australian Government agencies.

Key findings

24. The selected agencies were assessed on their: compliance with the top four mitigation strategies and related controls; maturity to effectively manage logical access and change management as part of normal business processes (IT general controls); observed compliance state as at 30 November 2013; and reported planned compliance state by 30 June 2014.

25. The ANAO's summary findings for each of the selected agencies are reported in the context of a matrix, which indicates agencies' overall level of protection against internal and external threats as a consequence of the steps

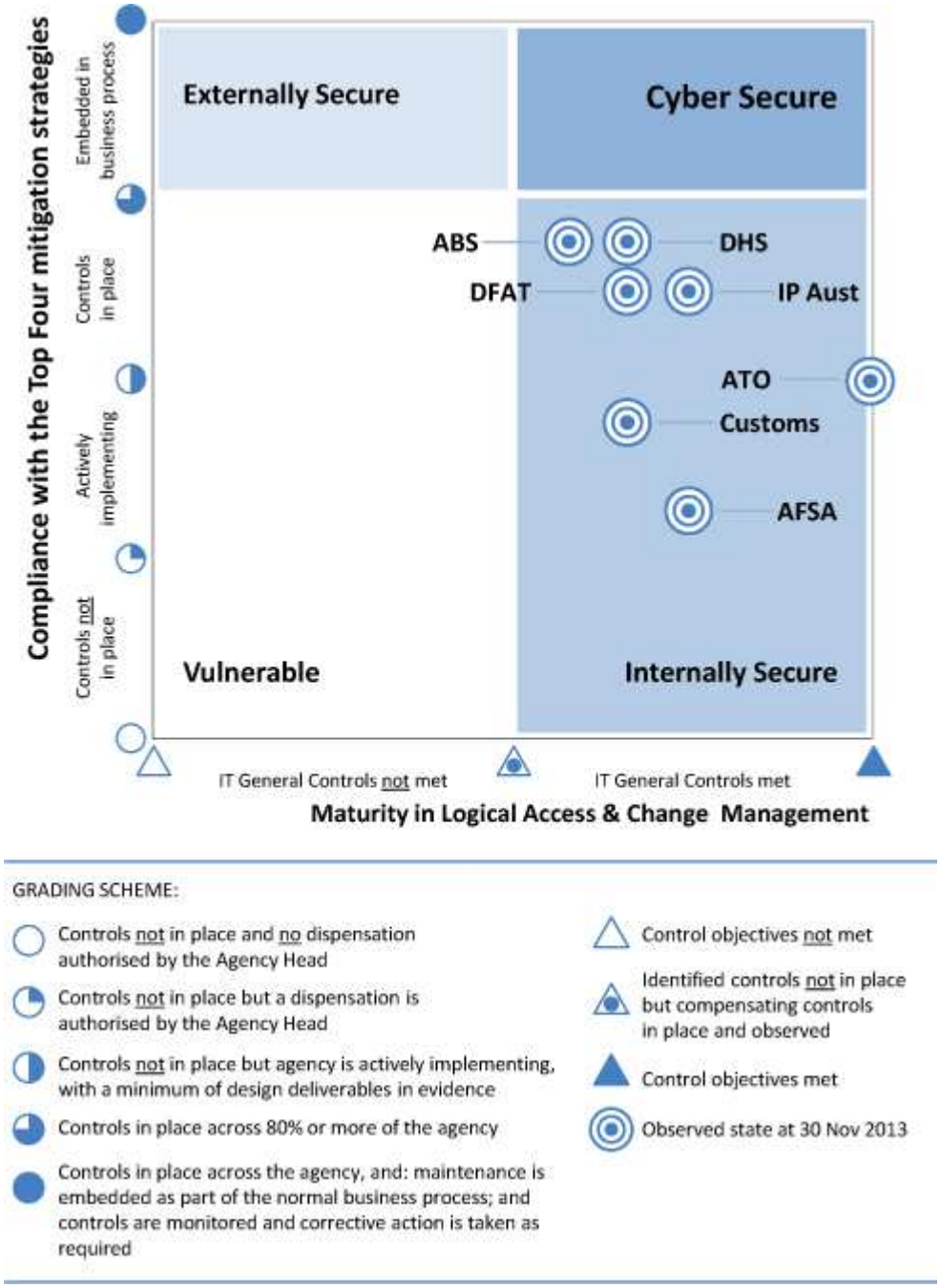
taken to implement the top four strategies and IT general controls. The matrix, which is referred to as the *Agency Compliance Grade,* indicates where agencies are positioned in terms of ICT security zones: *vulnerable* zone; *externally* secure zone; *internally* secure zone, and *cyber secure* zone. The zones are explained further in Table S.2 and illustrated in Figure S.1. An agency's position indicates its overall ICT security posture—in essence how well the agency is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

Table S.2: Definition of the ICT security zones

Zone scheme	Definition of the ICT security zones
Vulnerable Zone	High-level of exposure and opportunity for external attacks and internal breaches and disclosures of information
Externally Secure Zone	Reasonable level of protection from attacks and intrusions from external sources—but vulnerabilities remain to breaches and disclosures from internal sources
Internally Secure Zone	Reasonable level of protection from breaches and disclosures of information from internal sources—but vulnerabilities remain to attacks from external sources
Cyber Secure Zone	High-level of protection from external attacks and internal breaches and disclosures of information

Source: ANAO.

Figure S.1: Agency Compliance Grade: summary assessment of agencies' compliance with top four mandatory strategies and related controls, and overall ICT security posture



Source: ANAO. See Figure 2.3 for the agencies' planned state by 30 June 2014.

Note: IT General Controls are policies and procedures developed to deal with identified ICT system risks, including controls in relation to ICT governance, ICT infrastructure, security and access to operating systems and databases, and program change procedures.

26. In summary, each of the selected agencies was located in the *Internally Secure Zone*. The agencies had security controls in place to provide a reasonable level of protection from breaches and disclosures of information from internal sources. However, this is not sufficient protection against cyber attacks from external sources. To comply fully with the PSPF, agencies should also have a reasonable level of protection from external threats. The preferred state is for an agency to be located in the *Cyber Secure Zone*—where both ISM and IT general controls are effectively in place across the agency's enterprise systems, providing a high level of protection against all threats.

27. The selected agencies had not yet achieved full compliance with the PSPF and ISM, although each has advised of improvement activities underway.[16] Agencies further advised that factors affecting their current security posture and level of compliance with the four mandated strategies included: competing operational priorities[17]; resource restraints; and accessing specialist skills. In the context of working towards compliance with the mandated requirements, it is important that agencies develop a timetable and process to guide implementation.

Application whitelisting deployed on desktops and servers

28. Application whitelisting is a control which protects against unauthorised applications executing on a system. The ANAO observed that the deployment of application whitelisting across agency desktops was a priority activity for all agencies. Three of the seven agencies had implemented application whitelisting across the desktops, while one agency was also actively implementing application whitelisting across its servers.

29. The ANAO examined the application whitelisting rules used by each of the agencies—a set of protocols to identify executable files—and found that in most cases only simple rules were adopted.[18] The ANAO raised concerns when it observed, in the case of two agencies, that their application whitelisting was set to 'audit only mode', which simply logged events that application whitelisting would have blocked, had it been enabled. Both agencies immediately rectified this shortcoming. Of further concern, in the case of four agencies, was that the default policy was not set to deny the execution of software, potentially enabling staff without administration rights to load software on agency systems.

Policies and procedures for security patching of applications and operating systems

30. Security patching involves the periodic deployment of software releases designed to fix problems with existing software. The ANAO observed that while all agencies had implemented a patch management strategy, procedure or instruction that aligned with their change management procedures, these approaches were inadequate to cover the patching or upgrade of desktop and corporate applications to address known security vulnerabilities. More attention was given by agencies to the timely deployment of security patches to operating systems at the desktop and servers. All agencies had mitigating controls to prevent attacks or resolve issues to their systems where known vulnerabilities could not be patched.

31. In all cases, agencies were non-compliant with the requirements to apply critical security patches within two days from the release of the patches, and only two agencies had demonstrable patching practices enabling them to respond to vendors' routine or *ad hoc* patch releases, such as Microsoft's monthly security patch release. While there may be practical challenges to overcome in applying security patches within mandated timeframes, agencies will experience additional risk exposures the longer they delay implementation.

Management of standard and administrative privileged accounts

32. Administrative privileges are the highest level of permission, granted only to trusted personnel to enable them to configure, manage and monitor an ICT system. The ANAO reviewed agencies' group policies for account access, with attention given to the management of privileged accounts. For all agencies: administrative users held separate accounts to perform system administrative duties; were denied email accounts and Internet access; and privileged accounts were controlled and auditable. However, five of the selected agencies had shortcomings in processes used to capture and maintain audit logs for privileged user accounts, and there were also inconsistent practices across agencies in the administration of group policies.

33. Further, the ANAO's assessment of agency policies to capture and maintain audit logs for privileged user accounts, found that in most cases the policy was not enforced. This is a systemic control weakness that raises questions as to how effectively agencies can identify, respond to, or investigate unauthorised access to privileged user accounts, or inappropriate activities by privileged users.

IT general controls

34. The ANAO examined key components of the selected agencies' IT general controls, relating to logical security access and change management. The ANAO observed that the selected agencies, in general, had appropriate and effective access control and change management processes in place. An area for improvement that is relevant for most of the agencies is the access control requirements to the database layer.[19] While other layers of control compensate to varying degrees for weaknesses in this regard, this is an issue that requires early attention.

Agencies' planned improvement activities

35. The need for continuous disclosure and improvement are features of the Australian Government's protective security framework, with the PSPF requiring agencies to:

> Undertake an annual security assessment against the mandatory requirements detailed in the PSPF,

and report their compliance with the mandatory requirements to the relevant portfolio Minister.[20]

36. Australian Government agencies are required to use the PSPF compliance reporting process to inform their portfolio Minister(s) and the Attorney-General—who is responsible for national protective security policy and privacy—of progress against mandatory PSPF requirements, and any rationale for non-compliance. The ASD's top four mitigation strategies were mandated with effect from 2013, and must therefore be reported on by agencies. The first of the agencies' self-assessment compliance reports to include an assessment against the mandatory requirements were due in September 2013. However, this did not mean that agencies were expected to have successfully implemented the mandatory requirements by this time, and an 18 month implementation period was set.

37. The ANAO examined the self-assessment compliance reports, as submitted by each of the selected agencies. In all cases, agencies reported non-compliance for one or more of the mandatory requirements.

38. All agencies advised the ANAO of plans to implement further initiatives to strengthen security controls with a view to improving compliance with the PSPF and ISM. The ANAO assessed the selected agencies' plans to achieve compliance by 30 June 2014. Assessments were conducted for agency activities that were: underway by November 2013; had demonstrable design deliverables; and were assessed as having a low level of risk regarding deployment by 30 June 2014.

39. Each of the selected agencies has activities underway that if effectively and fully implemented, would strengthen ISM controls and enhance the level of protection of information and systems, by 30 June 2014. For six of the agencies, the strengthening of one or more of the ISM controls would improve their agency compliance grade. Notwithstanding the agency activities planned for implementation by 30 June 2014, and in the absence of further agency initiatives, all of the selected agencies are likely to remain in the *Internally Secure Zone* and not achieve full compliance with the mandatory ISM controls by 30 June 2014, the date specified by the Australian Government.

40. Where agencies are unable to comply fully with mandatory Government requirements within a specified timeframe, it is important that they develop a clear timetable and process to establish a path to compliance and guide implementation.

Strengthening agencies' ICT security posture

41. In the context of an evolving cyber threat environment, agencies must have cyber resilience, to enable them to continue providing services while also deterring and responding to external cyber attacks. A sound understanding of an agency's ICT security posture can provide senior management with assurance that effective security measures are implemented to reduce the risk posed by cyber attacks. While ICT operational staff retain day-to-day responsibility for setting and enforcing security policy and procedures across systems, governance arrangements commensurate with the threat, and informed by risk analysis, can provide additional assurance.

42. Security awareness and initiatives are a shared responsibility within an organisation. Well prepared agencies adopted a mutual obligation approach towards security awareness, responsibility and accountability; where key staff had a duty to monitor and report on observed cyber behaviour. Leading by example, senior managers in these agencies responded to cyber security incidents in a timely manner (reactive), and were informed of cyber trends—the motives, opportunities and emerging technology—that might target and compromise agency systems (proactive). To achieve this outcome, the relevant executives understood their roles and responsibilities to enhance security initiatives for the services they were accountable for, and tended not to expect ICT technical staff to be solely responsible for resolving ICT security matters.

43. Further, agencies which look beyond the four mandated strategies are better placed to manage threats and intrusions. Each of the selected agencies had taken varying steps to implement the remaining 31 controls from the *Top 35 mitigation strategies against cyber intrusions* promulgated by ASD.

Summary of agencies' responses

44. Agencies' summary responses to the audit report are provided below. Agency responses to each recommendation are included in the body of the report, directly following each recommendation. Formal responses from the agencies are included at Appendix 1.

Selected agencies' responses

Australian Bureau of Statistics

45. The ABS agrees that the report is an accurate assessment of the agency's compliance state as of 30 November 2013 and the agency's planned state for 30 June 2014.

46. The ABS supports the recommendations of the report and notes that the agency is well placed in terms of its compliance with the top four ISM controls.

47. The audit has identified some areas for improvement and the agency has established programs of work to implement these recommendations. Where full compliance has not been possible due to technical constraints imposed by a small number of legacy systems, mitigations have been put in place to reduce the risks associated with the use of these.

Australian Customs and Border Protection Service

48. The ACBPS believes your audit methodology and the resulting findings are fair and accurate based on the point-in-time of the field phase. The Service has and will continue to benefit from your contribution to our program of work and we look forward to the opportunity to engaging with your team and the other audit agencies to leverage each other's advancements.

49. The ACBPS is enhancing its security culture to address the growing cyber threat. Underpinned by clear policy, supported by security aware leadership the security team has a mandate to achieve compliance with the Australian Signals Directorate Top 35.

Australian Financial Security Authority

50. The Australian Financial Security Authority (AFSA) accepts the proposed report on *Cyber Attacks: Securing Agencies' ICT Systems,* and agrees with the Australian National Audit Office's assessment of agency systems. AFSA will continue in our efforts to achieve full compliance with the top four ASD strategies against potential cyber attacks.

51. AFSA acknowledges the importance of developing and implementing strategies and policies to strengthen the agency security posture. AFSA will continue to develop these strategies and policies in an informed manner so that we may achieve the optimal level of control over our systems to mitigate the risk of cyber attacks.

52. AFSA agrees with the recommendations contained in the report, and appreciates the recognition from the Australian National Audit Office relating to the works completed.

Australian Taxation Office

53. The Australian Taxation Office (ATO) welcomes the proposed audit report on *Cyber Attacks: Securing Agencies' ICT Systems*, and agrees with the Australian National Audit Office's overall assessment. The ATO remains committed to achieving full compliance with the top four mandated strategies against potential cyber-attacks.

54. The ATO will continue to develop and implement strong and robust strategies and policies to continually strengthen the security of ICT systems and achieve the desired level of control over our systems to mitigate the risk of cyber intrusions. The ATO agrees with the three recommendations contained in the report. Overall, the ATO appreciates the recognition given for the work undertaken to date.

The Department of Foreign Affairs and Trade

55. The Department of Foreign Affairs and Trade (DFAT) has reviewed the proposed report on *Cyber Attacks: Securing Agencies' ICT Systems*, dated 12th May 2014. DFAT agrees with the Australian National Audit Office's key findings and is working towards capability improvements that will increase the level of protection from external attacks and internal breaches and disclosure of information.

56. DFAT will continue to improve compliance with the top four mitigation strategies and related mandatory controls

to mitigate risks associated with cyber-attacks. Existing processes and security systems will be strengthened to protect the security of Australian Government information and systems. DFAT agrees with the three recommendations in the report and the value of the work performed in identifying areas for improvement.

The Department of Human Services

57. The Department of Human Services (the department) welcomes this report, and considers that the implementation of its recommendations will enhance our current work practices and our already strong compliance status.

58. The department takes its commitment to securing our organisation against cyber security attacks very seriously. The department will continue to strengthen the posture of compliance with the top four mandatory strategies, related controls and overall ICT security.

IP Australia

59. IP Australia welcomes this report and considers that implementation of the recommendations will enhance the security of its ICT systems. IP Australia agrees with the recommendations in the report and has in place a plan to further strengthen its capability in all these areas. An action plan to address compliance with the Top 4 Strategies is already underway and these recommendations will be added to that plan.

60. IP Australia has reviewed and is actively working to improve its security posture within a timeframe and resource envelope that can be managed based on its cost recovery model of operation. A risk based approach has been used to prioritise improvements to security and to ensure the highest vulnerabilities are addressed first. With its increase in online services, the increasing threat environment, and the increase in compliance requirements, IP Australia has increased ICT Security resources and initiatives to improve its overall security posture.

Other agency responses

61. A copy of the proposed audit report was also provided to the Attorney-General's Department (AGD) and the Australian Signals Directorate (ASD) for any comments they wished to make. The AGD provided informal comment in the drafting of this report. ASD's response is set out below.

Australian Signals Directorate

62. The Australian Signals Directorate (ASD) endorses the three recommendations of the Australian National Audit Office cross-agency audit report on Cyber Attacks: Securing Agencies' ICT Systems. This audit report is important for the selected agencies and others to improve their ICT security.

63. Based on ASD's technical and operational experience in cyber security, the Top 4 remain the most effective way to mitigate targeted cyber intrusions when implemented as a package. No single strategy can prevent a targeted cyber intrusion, and ASD encourages all government agencies to continue to make inroads into the application of the Top 4. Once organisations have effectively implemented the Top 4 mitigation strategies, ASD recommends additional mitigation strategies be selected from the remaining 31 to address security gaps until an acceptable level of residual risk is reached.

Recommendations

The recommendations are based on findings from fieldwork at the selected agencies, and are likely to be relevant to other agencies. Therefore, all agencies are encouraged to assess the benefits of implementing these recommendations in light of their own circumstances, including the extent to which each recommendation, or part thereof, is addressed by practices already in place.

Recommendation No. 1 **Paragraph 2.34**	To achieve full compliance with the mandatory ISM strategies and related controls, the ANAO recommends that agencies: (b) complete activities in train to implement the top four ISM controls across their ICT environments; and

	(c) define pathways to further strengthen application whitelisting, security patching for applications and operating systems, and the management of privileged accounts. **Response from selected agencies:***Agreed*
Recommendation No. 2 **Paragraph 4.63**	To reduce the risk of cyber attacks to information stored on agency databases, the ANAO recommends that agencies strengthen logical access controls for privileged user accounts to the database by eliminating shared accounts, recording audit logs and monitoring account activities. **Response from selected agencies:***Agreed*
Recommendation No. 3 **Paragraph 5.23**	To strengthen their ICT security posture, the ANAO recommends that agencies: (a) conduct annual threat assessments across the ICT systems, having regard to the *Top 35 Mitigations Strategies*—as proposed by the Australian Signals Directorate; and (b) implement periodic assessment and review by the agency security executive of the overall ICT security posture. **Response from selected agencies:***Agreed*

Contact

David Gray, Executive Director - Phone (02) 6203 7377

[1] National cyber security expenditure was approximately $480 million in 2011–12, representing approximately 13.9 per cent of Australian Government Homeland and Border security expenditure. See Department of the Prime Minister and Cabinet, *Strong and Secure: A strategy for Australia's National Security*, 2013, p. 15.

[2] The most recent Australian survey on cyber risks to business indicates that some 56 per cent of organisations identified cyber security incidents on their networks in 2013, compared to 22 per cent in 2012, an increase of 34 per cent. See Attorney-General's Department, CERT Australia, *Cyber Crime & Security Survey Report 2013*, p. 5.

[3] Until 2013, ASD was known as the Defence Signals Directorate (DSD). To avoid confusion, it will be referred to as ASD throughout this audit report.

[4] The Centre, established in ASD, has two main roles: to provide government with a better understanding of sophisticated cyber threats against Australian interests; and to coordinate and assist operational responses to cyber events of national importance across government and systems of national importance.

[5] The scale and sophistication of cyber attacks against government and private sector systems has increased significantly, with ASIO highlighting in 2012–13 the threats posed to national security and economic competitiveness by cyber activity, espionage through electronic means, and the unauthorised use of sensitive material by trusted employees. See Australian Security Intelligence Organisation, *ASIO Report to Parliament 2012–2013* [Internet], available from <http://www.asio.gov.au> [accessed on 4 November 2013].

[6] In essence how well the agency is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

[7] The PSPF was first released in June 2010, with several subsequent amendments. In April 2013, the PSPF was updated to include four mandatory strategies and related controls to mitigate targeted cyber intrusions.

[8] The ISM complements the PSPF, and is an important part of the Australian Government's strategy to enhance its information security capability.

[9] Defence Signals Directorate, *Application whitelisting explained* [Internet], 2012, available from

<http://www.dsd.gov.au/publications/csocprotect/application_whitelisting.htm> [accessed 23 May 2013]. Defining a list of trusted executables—a whitelist—is a more practical and secure method of securing a system than prescribing a list of bad executables to be prevented from running—a blacklist.

[10] Defence Signals Directorate, *Assessing security vulnerabilities and patches* [Internet], 2012, available from <http://www.dsd.gov.au/publications/csocprotect/assessing_security_vulnerabilities_and_patches.htm> [accessed 23 May 2013]. A patch is a piece of software designed to fix problems with, or update, a computer program or its supporting data; this includes fixing security vulnerabilities.

[11] Defence Signals Directorate, *Minimising administrative privileges explained,* 2012, available from <http://www.dsd.gov.au/publications/csocprotect/minimising_admin_privileges.htm> [accessed 23 May 2013]. System administrators typically have greater access rights to systems and information than normal users.

[12] Similarly, CERT Australia advises business to use the Top Four mitigation strategies. CERT Australia is the national computer emergency response team within AGD, which works with major Australian businesses to provide cyber security advice and support to critical infrastructure and other systems of national interest. See Attorney-General's Department, CERT Australia, *Cyber Crime & Security Survey Report 2013*, p. 20.

[13] The guidelines contain the underlying principles and outline the responsibilities that agencies are required to follow when measuring their compliance against the PSPF mandatory requirements. See Attorney-General's Department, *Protective security governance guidelines–Compliance reporting* [Internet], 2012, available from <http://www.protectivesecurity.gov.au/governance/audit-reviews-and-reporting/Pages/Supporting-guidelines-for-audit-reviews-and-reporting.aspx> [accessed 17 June 2013].

[14] These are logical access and change management controls. Logical access controls prevent unauthorised access to ICT resources (including files, data and applications) and the associated administrative procedures. Change management controls ensure that standardised methods and procedures support the formal request for a change to ICT systems.

[15] ANAO Audit Report No.49 2013–14, *The Management of Physical Security.*

[16] Figure 2.3 illustrates the selected agencies' observed compliance state at 30 November 2013, and the planned compliance state by 30 June 2014.

[17] For example, ICT resources must be allocated to deliver a range of business outcomes.

[18] Specifically, simple certificate and folder based rules were adopted.

[19] The database layer is where official information resides on an IT system.

[20] In accordance with the guidance set out in the PSPF, this reporting should be incorporated with the compliance reporting against other PSPF requirements and should be sent to: the relevant portfolio Minister; the Secretary of the Attorney-General's Department; and the Auditor-General for Australia.
