5

Performance Audit Report No. 50 (2013-14)

Cyber Attacks: Securing Agencies' ICT Systems

Introduction

5.1 Chapter 5 discusses the Joint Committee of Public Accounts and Audit (JCPAA) review of the Australian National Audit Office (ANAO) Report No. 50 *Cyber Attacks: Securing Agencies' ICT Systems*. The chapter comprises:

- an overview of the report, including audit objective, criteria and scope, audit conclusion and audit recommendations
- Committee review
- Committee comment

Background

5.2 The protection of Australian government information communications and technology (ICT) systems and data is an important responsibility of all Commonwealth agencies. The Australian Signals Directorate (ASD) estimated that, between January and December 2012, there were over 1790 security incidents against Australian government agencies. Of these

security incidents, 685 were considered serious enough to warrant a response from the Cyber Security Operations Centre (CSOC).[1]

5.3 Agencies are required to have effective protective security arrangements in place to ensure that the functional capacity of the agency and 'official resources and information the agency holds in trust, both from and for the public, and those provided in confidence by other countries, agencies and organisations, are safeguarded.'[2]

5.4 The Attorney General's Department (AGD) is responsible for the development and refinement of the *Protective Security Policy Framework* (PSPF) that 'promotes the most efficient and effective ways to secure the continued delivery of Government business.'[3]ASD is responsible for the production of the *Australian Government Information Security Manual* (ISM). The ISM is the standard which governs the security of government information and ICT systems; it complements the PSPF.[4]

5.5 In 2010, ASD developed a list of 35 strategies to assist agencies to achieve the desired level of control over their ICT systems and mitigate the risk of cyber intrusions. ASD advised that, if fully implemented, the top four mitigation strategies would prevent at least 85 per cent of targeted cyber intrusions to an agency's ICT systems. In April 2013, the PSPF was amended, mandating the full implementation of the top four mitigation strategies by July 2014.[5]

5.6 In November 2014, the Prime Minister announced a review of Australia's cyber-security strategy 'to better protect Australia's networks from cyber attack.' The review, which is expected to report before May 2015, 'will explore how industry and government can work together to make our online systems more resilient against attacks. The Cyber Security Review will be led by the Department of Prime Minister and Cabinet and be assisted by a panel of experts.[6]

---

1 ANAO, Audit Report No. 50 (2013-14), *Cyber Attacks: Securing Agencies' ICT Systems*, p. 12.

2 Attorney General's Department (AGD), 'Directive on the security of Government business', *Protective Security Policy Framework* (PSPF) <http://www.protectivesecurity.gov.au/pspf/Pages/Directive-on-the-security-of-Government-business.aspx> accessed 26 November 2014.

3 AGD, 'Directive on the security of Government business', PSPF, accessed 26 November 2014.

4 Australian Signals Directorate (ASD), *Information Security Manual* (ISM) <http://www.asd.gov.au/infosec/ism/> accessed 5 November 2014.

5 ANAO, Audit Report No. 50 (2013-14), pp. 13-14.

6 Mr Tony Abbott MP, Prime Minister of Australia, 'Cyber Security Review' Media Release, 27 November 2014, < https://www.pm.gov.au/media/2014-11-27/cyber-security-review-0> accessed 1 December 2014.

Report Overview

Audit objective, criteria and scope

5.7 The audit objective was to assess selected agencies' compliance with the mandatory top four mitigation strategies and related controls in the ISM, as well as considering agencies' overall security posture. In addition, the audit assessed the accuracy of agencies' self-assessment reports regarding compliance against the ISM controls.[7]

5.8 The mitigation strategies audited were:

- application whitelisting
- patching applications
- patching operating systems
- minimising administrative privileges

5.9 The following seven agencies were selected by the ANAO:

- 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)
- IP Australia[8]

5.10 The agencies were selected based on the character and sensitivity of the information managed by the agency. This is summarised in Table 5.1.

Table 5.1 Key information collected, stored and used by the selected agencies

Agency	Economic information	Policy and regulatory information	National security information	Program and service delivery	Personal information
ABS	♦				♦
Customs			♦	♦	♦
AFSA	♦	♦			♦
ATO	♦	♦			♦
DFAT	♦	♦	♦	♦	♦
DHS				♦	♦
IP Australia		♦		♦	

7 ANAO, Audit Report No. 50 (2013-14), p. 16.

8 ANAO, Audit Report No. 50 (2013-14), p. 15.

Source ANAO Audit Report No. 50 (2013-14), p. 15.

Audit conclusion

5.11 The audit found that the selected agencies had not yet achieved full compliance with the mandatory top four mitigation strategies and that none of the selected agencies was expected to achieve full compliance by the target date of July 2014.[9]

5.12 The ANAO found that the selected agencies' overall ICT security posture provided a 'reasonable level of protection from breaches and disclosures of information from internal sources,' but that there were, 'vulnerabilities remaining against attacks from external sources'.[10] The ANAO commented that '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.'[11]

Audit recommendations

5.13 Table 5.2 sets out the recommendations for Audit Report No. 50 (2013-14).

Table 5.2 ANAO recommendations – Audit Report No. 50 (2013-14)

1	To achieve full compliance with the mandatory ISM strategies and related controls, the ANAO recommends that agencies: a. complete activities in train to implement the top four ISM controls across their ICT environments; and b. define pathways to further strengthen application whitelisting, security patching for applications and operating systems, and the management of privileged accounts. **Selected agencies' response**: *Agreed*.
2	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. **Selected agencies' response**: *Agreed*.
3	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 Mitigation 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. **Selected agencies' response**: *Agreed*.

Source ANAO Audit Report No. 50 (2013-14), pp. 29-30.

9 ANAO, Audit Report No. 50 (2013-14), p. 17.

10 ANAO, Audit Report No. 50 (2013-14), p. 18.

11 ANAO, Audit Report No. 50 (2013-14), p. 18.

5.14 Due to the risk of disclosing sensitive information about agency ICT systems, the ANAO departed from its usual practice of identifying agencies on individual issues and instead addressed security weaknesses at an aggregate level.[12] The ANAO presented its findings in the context of a matrix which indicated 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 ANAO referred to this matrix as the *Agency Compliance Grade*; it can be found below at Figure 5.1.[13] The *Agency Compliance Grade* indicates where agencies are positioned in terms of ICT security zones; the zones are explained below in Table 5.3.

Table 5.3 Definition of ICT security zones

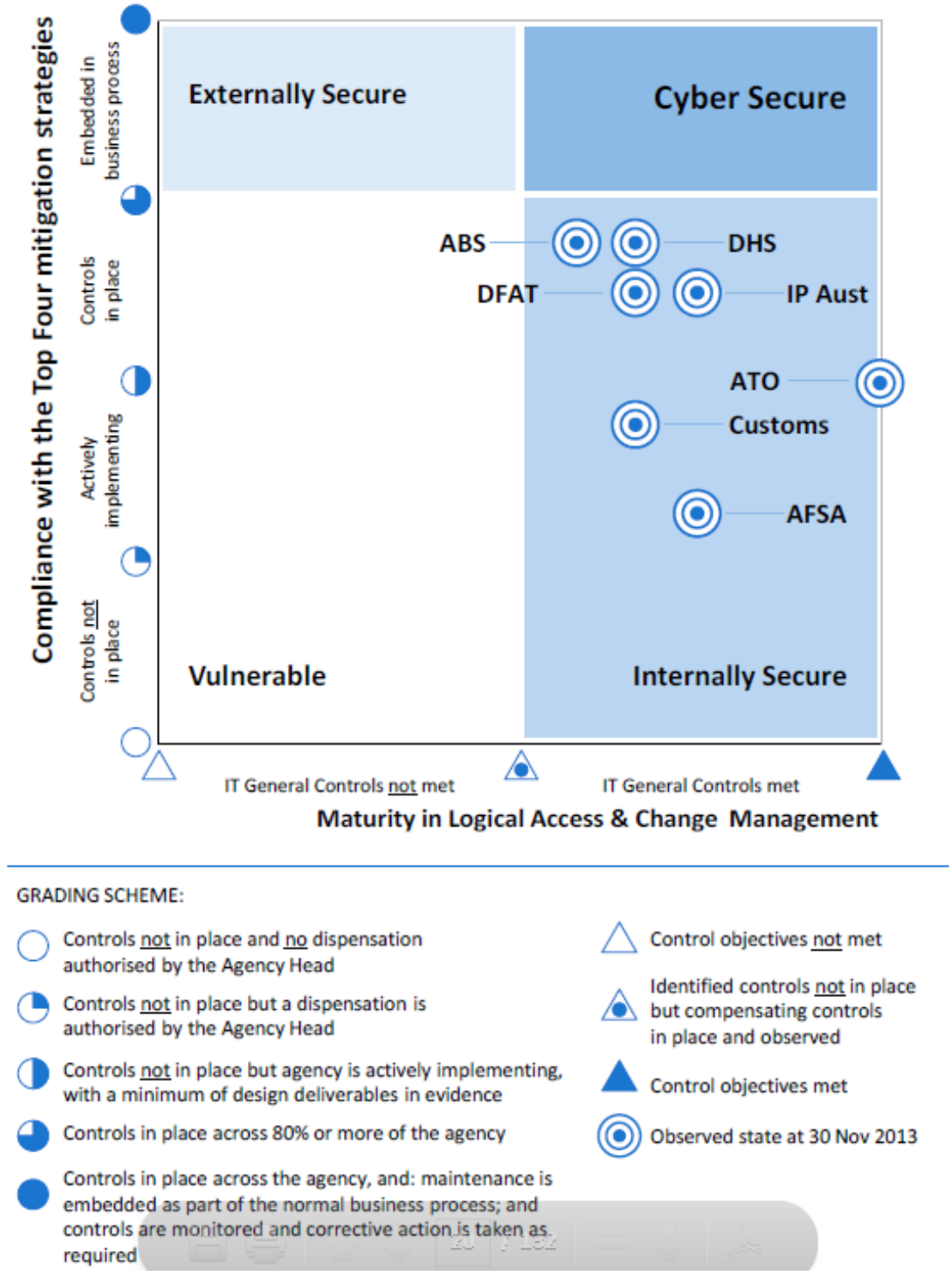
Zone Scheme	Definition of ICT security zones
Vulnerable Zone	High-level exposure and opportunity for external attacks and internal breaches and disclosures of information. • Systemic weakness across the ICT environment relating to protection of information and systems from external attacks and internal breaches and disclosures. • ISM and IT general controls not in place, or inconsistently implemented across the system.
Externally Secure Zone	Reasonable level of protection from attacks and intrusions from external sources – but vulnerabilities remain to breaches and disclosures from internal sources. • Top Four ISM strategies and replated controls in place across 80% or more of the agency's ICT systems and are embedded in (or working towards) business processes.
Internally Secure Zone	Reasonable level of protection from breaches and disclosures of information from internal sources – but vulnerabilities remain to attacks from external sources. • IT general controls from logical access and change management are met by the agency.
Cyber Secure Zone	High-level protection from external attacks and internal breaches and disclosures of information. • Top Four ISM strategies and related controls in place across 80% or more of the agency's ICT systems and IT general controls for logical access and change management are met by the agency.

Source ANAO Audit Report No. 50 (2013-14), p. 49.

12 ANAO, Audit Report No. 50 (2013-14), p. 45.

13 ANAO, Audit Report No. 50 (2013-14), p. 19.

Figure 5.1 Agency Compliance Grade: summary assessment of agencies' compliance with top four mandatory strategies and related controls, and overall ICT security posture



Source *ANAO Audit Report No. 50 (2013-14), p. 20.*

Committee review

5.16 The ANAO report stated that the unauthorised access and misuse of government information can have wide-reaching impacts on national security, the economy, personal privacy, and the integrity of data holdings. As such, the protection of ICT systems and information, from both internal and external security risks, is a key responsibility of government agencies.[14]

5.17 The ANAO found that, whilst the security controls of the selected agencies provided a reasonable level of protection from breaches and disclosures of information from internal sources, agencies did not have sufficient protection against cyber attacks from external sources[15] (see also Figure 5.1).

5.18 The Committee focused on several areas of interest:

- compliance with the top four mitigation strategies
- IT general controls
- planned improvement activities
- improving security posture
- accountability and reporting

Compliance with top four mitigation strategies

5.19 The ANAO found that the selected agencies had not achieved full compliance with the mandated top four mitigation strategies at the time of audit, and were not expected to achieve full compliance by the target date of July 2014.[16] The four strategies – application whitelisting; patching applications, patching operating systems; and administrator privileges – are discussed below.

Application whitelisting

5.20 Application whitelisting is a control that protects a system from unauthorised applications. The ISM advises that an application whitelist (a list of trusted executables[17]) is a more practical and secure method of securing a system than an application blacklist (a list of bad executables to be prevented from running).[18] The ISM states that application whitelisting

14 ANAO, Audit Report No. 50 (2013-14), p. 17.

15 ANAO, Audit Report No. 50 (2013-14), p. 21.

16 ANAO, Audit Report No. 50 (2013-14), p. 81.

17 An executable is a file that runs a program when it is opened; it executes code or a series of instructions contained in the file.

18 ASD, *2014 Australian Government Information Security Manual: Controls*, p. 164.

is 'an effective mechanism to prevent the compromise of a system resulting from the exploitation of vulnerabilities in an application or from the execution of malicious code.'[19]

5.21 The ANAO noted that the deployment of application whitelisting across desktops was a priority activity for all of the selected agencies. The ANAO found that, of the seven agencies:

- five agencies had application whitelisting strategies, policies and rules in varying states
- three agencies had implemented whitelisting across their desktop systems
- two agencies were actively deploying strategies for their desktop systems
- one agency was actively implementing application whitelisting across its servers.[20]

5.22 The ANAO commented that application whitelisting was 'in general hastily deployed by agencies', with some agencies using 'audit only mode' to record executables in use across the system and that:

> Agencies did not tend to review and remove unauthorised executables, which is the better practice approach. The agencies adopted file path-based rules to enforce policy, which is the 'weakest' of the available rules to secure a whitelist.[21]

Patching applications and operating systems

5.23 Security patching[22] involves the periodic deployment of software releases designed to fix problems with existing software. The ISM states that 'applying patches to operating systems, applications and devices is a critical activity in ensuring the security of systems.'[23] It is rated by the ASD as one of the most effective security practices that an agency can perform.[24]

5.24 Security patches should be deployed within a timeframe that is proportionate with the severity of the threat/risk. The ISM states that agencies must apply all security patches as soon as possible and that for security vulnerabilities assessed as 'extreme risk' agencies must apply the

19 ASD, *2014 Australian Government Information Security Manual: Controls*, p. 164.

20 ANAO, Audit Report No. 50 (2013-14), p. 64.

21 ANAO, Audit Report No. 50 (2013-14), p. 81.

22 A patch is a piece of computer code that is inserted into an existing program to fix problems or to improve usability and performance.

23 ASD, *2014 Australian Government Information Security Manual: Controls*, p. 158.

24 ASD, *2014 Australian Government Information Security Manual: Controls*, p. 158.

security patch or mitigate the vulnerability (if there is no patch available) within two days.[25]

5.25 The following deployment timeframes for security patches are recommended by the ASD, based on risk:

- extreme – within 48 hours
- high – within two weeks
- medium – within three months
- low – within one year[26]

5.26 The ANAO noted that 'a responsive and effective security patch strategy relies on a lifecycle of: preparedness; vulnerability identification and patch acquisition; risk assessment and prioritisation; patch testing and deployment; and verification.'[27]

Patching applications

5.27 The ANAO found that three of the seven agencies did not deploy any security patches for applications between May to August 2013, during 2013, or since the last upgrade of the applications sampled by the ANAO; whilst another three agencies conducted security patching on an '*ad hoc* basis'. The ANAO found that only one agency consistently deployed security patches for the sampled applications whilst also remaining within the vendors' recommended timeframe based on the threat assessment.[28]

5.28 Agencies reported difficulties in patching or installing the latest version of an application within the required two day timeframe. The ANAO reported that:

> Agencies expressed concerns about the risk of hastily upgrading an application into the production environment without a comprehensive systems test – a test and release cycle that usually required a much longer time period than two days.[29]

5.29 The ANAO acknowledged that there may be practical challenges to overcome in applying security patches to applications, but that, despite this, agencies will experience additional risk exposures the longer they delay implementation.[30]

---

25 ASD, *2014 Australian Government Information Security Manual: Controls*, p. 159.
26 ANAO, Audit Report No. 50 (2013-14), p. 70.
27 ANAO, Audit Report No. 50 (2013-14), p. 82.
28 ANAO, Audit Report No. 50 (2013-14), p. 71.
29 ANAO, Audit Report No. 50 (2013-14), p. 72.
30 ANAO, Audit Report No. 50 (2013-14), p. 73.

Patching operating systems

5.30 The ANAO found that four of the seven agencies deployed security patches for operating systems within the timeframes recommended by ASD. The three other agencies advised that they used alternative patching practices due to:

- lack of regular maintenance windows for server environments
- competing business and 24/7 operations activities
- a preference to upgrade the operating system in the context of the next release version and when systems and integration testing has been completed by the agency.[31]

5.31 The ANAO found that all of the selected agencies conducted risk assessments and scheduled the deployment of the latest version of the operating system, for either desktops or servers, within the ASD's recommended timeframes.[32]

5.32 Overall, the ANAO commented that 'while the selected agencies understood the importance of adhering to a patching strategy and policy, they generally adopted an *ad hoc* approach to applying the lifecycle.'[33]

Administrator privileges

5.33 Administrative privileges are the highest level of permission and allow users to configure, manage and monitor a system. A user with administrative privileges can make any change and retrieve almost any information from a system.[34] The risks this poses are noted in the ISM, which states that 'privileged accounts are targeted by adversaries as these can potentially give full access to the system.'[35]

5.34 The ISM prescribes that administrative privileges should be allocated to separate administrative accounts, which should be controlled, logged, monitored and auditable. These accounts, and the level of privileges attached to each, should be limited to only those users who require them and the passphrases for the accounts should be audited regularly. Furthermore privileged accounts must not be allowed access to the internet or email.[36]

5.35 The ANAO found that user access rights were governed by documented policies, which considered job requirements and business needs, in all of

31 ANAO, Audit Report No. 50 (2013-14), p. 75.
32 ANAO, Audit Report No. 50 (2013-14), p. 76.
33 ANAO, Audit Report No. 50 (2013-14), p. 82.
34 ANAO, Audit Report No. 50 (2013-14), p. 77.
35 ASD, *2014 Australian Government Information Security Manual: Controls*, p. 159.
36 ASD, *2014 Australian Government Information Security Manual: Controls*, pp. 201-201.

the selected agencies. However, in all cases, the ANAO observed that practices to restrict privileged accounts access did not align with agency policies, resulting in non-compliance with the ISM.[37] The ANAO also found that agency practices regarding passphrases for privileged user accounts did not align with agency policies, resulting in non-compliance with the ISM.[38]

5.36 The ANAO found that all of the selected agencies had separate accounts for administrative and standard use. However, one agency used shared administrator accounts for a database group policy. The agency advised the ANAO that it did this because it was more efficient to share an account amongst the ICT team for routine system maintenance work. However, the ANAO noted that the agency did not have a method of attributing actions undertaken by such accounts to specific personnel, which impacted upon accountability and 'introduced a high and avoidable level of risk.'[39]

5.37 The ANAO commented that, in the case of privileged user accounts, such as those with administration rights over IT systems, 'audit logs were captured to facilitate monitoring and accountability.'[40] However, the ANAO noted that 'agencies invested little or no effort in monitoring or reviewing the logs of actions by privileged users.'[41]

IT general controls

5.38 IT general controls refer to the policies and procedures that address an agency's identified system risks. This can include: controls over ICT governance; ICT infrastructure; security and access to operating systems and databases; application acquisition and development; and program change procedures.[42] The ANAO noted the importance of IT general controls, stating that:

> An effective IT general controls framework is an essential prerequisite for securing systems against cyber attacks. It creates layers of protection for critical systems elements against internal source threats and establishes a foundation for implementing controls directed against external source threats, including the mandated ISM strategies and related controls.[43]

37 ANAO, Audit Report No. 50 (2013-14), pp. 79-80.
38 ANAO, Audit Report No. 50 (2013-14), p. 81.
39 ANAO, Audit Report No. 50 (2013-14), pp. 79-80.
40 ANAO, Audit Report No. 50 (2013-14), p. 82.
41 ANAO, Audit Report No. 50 (2013-14), p. 82.
42 ANAO, Audit Report No. 50 (2013-14), p. 83.
43 ANAO, Audit Report No. 50 (2013-14), p. 83.

5.39 The ANAO found that agencies' logical access control and change management processes were, 'generally well positioned to deal with internal source threats,'[44] but noted that most of the agencies could improve the control of access to databases. The ANAO commented that:

> While other layers of control can compensate for weaknesses in this regard to some extent, this is an issue that requires early attention, so as to reduce the risk of external attacks and internal breaches and disclosures of information stored on agency databases.[45]

Planned improvement activities

5.40 The ANAO assessed the selected agencies' plans to achieve compliance by July 2014. The ANAO assessed activities that were underway by November 2013; had demonstrable design deliverables; and were assessed as having a low level of risk regarding deployment by July 2014.[46]

5.41 The ANAO found that, even when taking these planned improvement activities into consideration, none of the selected agencies was likely to achieve full compliance with the mandatory ISM controls by July 2014.[47] The ANAO presented its findings, comparing each agency's observed compliance grade and planned state, on page 56 of the ANAO Report.

5.42 The Committee sought an update from some of the selected agencies regarding when agencies expected to have cyber security embedded in their business processes. Mr Stephen Haywood, National Manager for Security, Risk and Assurance Branch, Customs assured the Committee that they have a framework in place, stating that:

> We have dedicated resources to things like patching. We have a 'vulnerability board' that meets monthly, around managing that risk around patching, which is ongoing. We report to the CEO on a monthly basis. So I think that we have that in place now, and certainly we are in a better position than we were.[48]

5.43 The ATO stated that:

> Out of the four mandatory controls – the top four – we are expecting to be compliant with the whitelisting one by the end of this year; we will be substantially compliant in patching, based on a risk based approach, mid-next year; and through access controls,

44 ANAO, Audit Report No. 50 (2013-14), p. 99.

45 ANAO, Audit Report No. 50 (2013-14), p. 99.

46 ANAO, Audit Report No. 50 (2013-14), p. 57.

47 ANAO, Audit Report No. 50 (2013-14), p. 57.

48 Mr Stephen Haywood, Customs, *Committee Hansard*, Canberra, 24 October 2014, p. 19.

> once again, substantially compliant and embedded in our business processes by mid-next year.[49]

5.44 DHS stated that:

> Human Services have committed to complete the whitelisting. We are compliant on the desktops but we have some technical difficulties with the Unix Solaris service…we have committed to do the access control by 2015 and the patching by 2016.[50]

5.45 The ANAO reported that the selected agencies advised of a number of factors affecting their security posture and level of compliance with the mandatory four mitigation strategies, including:

- competing operational priorities
- resource restrains
- accessing specialist skills[51]

5.46 Major General Stephen Day, Deputy Director, Cyber and Information Security, ASD, advised the Committee that the selected agencies' inability to achieve compliancy by July 2014 was not surprising:

> The view that the top four might be implemented by the middle of this year was, I would offer, optimistic. I think that all agencies have started implementing them, but some have got systems that do not allow some of those mitigation measures to be put in place. Defence, for example, will have to totally redo its operating system, and that will take some years…[The findings] did not surprise me and I think it will take some years before we are at a relatively mature state.[52]

5.47 DHS highlighted the challenge of implementing patches without compromising the quality and consistency of its services:

> You cannot patch your operating system unless you have patched your database, unless you have patched your application. Given that we in Human Services, in an active 24/7 shop, we cannot just take everything down and patch. We have to take this very carefully and very slowly through the patching levels.[53]

---

49 Mr Daniel Keys, Assistant Commissioner, Enterprise Solutions and Technology, Australian Taxation Office, *Committee Hansard*, Canberra, 24 October 2014, p. 19.

50 Mr Gary Sterrenberg, Chief Information Officer, DHS, *Committee Hansard*, Canberra, 24 October 2014, p. 19.

51 ANAO, Audit Report No. 50 (2013-14), p. 52.

52 Major General Stephen Day, Deputy Director, Cyber and Information Security, ASD, *Committee Hansard*, Canberra, 24 October 2014, p. 15.

53 Mr Gary Sterrenberg, Chief Information Officer, DHS, *Committee Hansard*, Canberra, 24 October 2014, p. 19.

5.48 The ANAO acknowledged that agencies may experience practical issues, but reaffirmed the importance of defining clear pathways through the problems and adopting a prudent, risk-based approach whilst seeking to achieve full compliance.[54]

Improving agencies' security posture

5.49 Security posture is defined by the ANAO as agencies' 'exposure to external and internal threats and vulnerabilities – and how well they are positioned to address threats and vulnerabilities.'[55] The agencies' compliancy grades (see Figure 5.1) reflect their ICT security posture as at November 2013, illustrating the individual agencies' exposure to cyber attacks and their readiness to combat cyber threats.[56]

5.50 The ANAO found that, based on their stage of implementation of the top four mitigation strategies and IT general controls, the selected agencies' overall ICT security posture provided:

> 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.[57]

5.51 The ANAO stated that security awareness and initiatives are a 'shared responsibility' and that well prepared agencies, 'adopted a mutual obligation approach towards security awareness, responsibility and accountability.'[58] The ANAO highlighted the importance of an agency's internal security culture:

> You need to have the right internal culture within the entity so that everybody is pulling together and it is not just the security people – those tasked day to day with security responsibilities – trying to operate a system on their own…it is almost axiomatic that when you have people pulling together internally they are more security aware. You are likely to have a better outcome, it is fair to say.[59]

5.52 The ANAO noted that, although there is no mandatory requirement that senior management of a particular level be involved in ICT security, all

---

54 Dr Tom Ioannou, Group Executive Director, Performance Audit Services Group, ANAO, *Committee Hansard*, Canberra, 24 October 204, p. 19.

55 ANAO, Audit Report No. 50 (2013-14), p. 101.

56 ANAO, Audit Report No. 50 (2013-14), p. 101.

57 ANAO, Audit Report No. 50 (2013-14), p. 18.

58 ANAO, Audit Report No. 50 (2013-14), p. 25.

59 Dr Tom Ioannou, Group Executive Director, Performance Audit Services Group, ANAO, *Committee Hansard*, Canberra, 24 October 204, p. 17.

agencies have a requirement for a head of security and a head of IT security.[60]

Cyber Security Operations Centre

5.53 The Cyber Security Operations Centre (CSOC) was established as an initiative of the Defence White Paper to mitigate the cyber threat to Australia's national security.[61] The CSOC is administered by ASD and is answerable to the Cyber Security Operations Board (CSOB), a secretary-level board chaired by the Attorney-General's Department.[62] The CSOC brings together the resources and expertise of a range of government agencies:

> It has the cybersecurity capabilities from the ASD, it has the Cyber Espionage Branch from ASIO [Australian Security Intelligence Organisation] there, it has the Computer Emergency Response Team from the Attorney-General's Department in there and it has elements of the Australian Federal Police and the Australian Crime Commission as well. In other words, it is pooling together the nation's key cybersecurity capabilities.[63]

5.54 The CSOC has the capacity to provide 'close and personal assistance' to 'make a real difference' to approximately 10 agencies per year. The CSOB has selected approximately 40 government organisations – based on their function, the information they collect, their attraction to foreign intelligence services – and categorised them into high, medium and low risk.[64]

5.55 The CSOC works in partnership with secretaries and SES officers to examine an agency's systems, providing tailored and ongoing advice as they work to improve their systems. The Secretary of AGD, together with one or two officers from the intelligence community, meet with the secretaries and SES officers of agencies that have been categorised as 'high risk' to 'explain the threat'.[65]

---

60 Dr Tom Ioannou, Group Executive Director, Performance Audit Services Group, ANAO, *Committee Hansard*, Canberra, 24 October 204, p. 17.

61 ASD, Cyber Security Operations Centre, <http://www.asd.gov.au/infosec/csoc.htm>, accessed 12 November 2014.

62 Major General Stephen Day, Deputy Director, Cyber and Information Security, ASD, *Committee Hansard*, Canberra, 24 October 2014, p. 15.

63 Major General Stephen Day, Deputy Director, Cyber and Information Security ASD, *Committee Hansard*, Canberra, 24 October 2014, p. 15.

64 Major General Stephen Day, Deputy Director, Cyber and Information Security, ASD, *Committee Hansard*, Canberra, 24 October 2014, p. 15.

65 Major General Stephen Day, Deputy Director, Cyber and Information Security, ASD, *Committee Hansard*, Canberra, 24 October 2014, p. 15.

Accountability and reporting

5.56 The PSPF Mandatory Requirement GOV-7 requires 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. In addition to reporting to their portfolio Minister, agencies are required to provide a copy of this report to the AGD and the ANAO. [66]

5.57 Agencies must also advise any non-compliance with mandatory requirements to: ASD, for matters relating to the ISM; Australian Security Intelligence Organisation (ASIO), for matters relating to national security; and the heads of any agencies whose people, information or assets may be affected by the non-compliance.[67]

5.58 The ANAO examined the selected agencies' self-assessment compliance reports and found that, in all cases, agencies reported non-compliance for one or more of the mandatory requirements.[68] Five of the seven agencies reported their compliance against each specific control in a narrative statements and/or a 'traffic light' report. Two of the agencies made general statements of compliance against the information security requirements in the PSPF.[69]

5.59 ASD and AGD work together to assess and report on Commonwealth agencies' implementation of the top four controls and their overarching strategies. Furthermore, ASD intends to conduct annual surveys, collating detailed information from agencies to assist agencies to meet reporting requirements.[70]

Reporting Breaches

5.60 The PSPF Mandatory Requirement GOV-8 requires agencies to ensure they have appropriate procedures for reporting and investigating security incidents and taking corrective action, in accordance with the provisions of the *Australian Government protective security governance guidelines – Reporting incidents and conducting security investigations*.[71] These guidelines 'amplify the PSPF governance requirements relating to incident reporting

66 AGD, *Securing Government Business: Protective security guidance for executives*, version 1, 21 October 2014, http://www.protectivesecurity.gov.au/pspf/Pages/SecuringGovernmentBusinessProtectiveSecurityGuidanceforExecutives.aspx accessed 26 November 2014, p. [12].

67 AGD, *Securing Government Business: Protective security guidance for executives*, p. [12].

68 ANAO, Audit Report No. 50 (2013-14), p. 24.

69 ANAO, Audit Report No. 50 (2013-14), p. 55.

70 ASD, *2014 Australian Government Information Security Manual: Controls*, p. 121.

71 AGD, *Securing Government Business: Protective security guidance for executives,* p. [12].

and investigative procedures and better practice that agencies should apply to meet the requirements of GOV-8.'[72] The guidelines state that:

> Agencies are required to report suspected cyber security incidents to [ASD] including:
>
> - suspicious or seemingly targeted emails with attachments or links
> - any compromise or corruption of information
> - unauthorised hacking
> - any viruses
> - any disruption or damage to services or equipment, and
> - data spills.[73]

5.61 Major General Day told the Committee that last year approximately 2,100 attempts against government systems were reported to or detected by the CSOC.[74]

Agency reporting policies

5.62 The Committee asked some of the selected agencies to outline their reporting policies and processes following either an internal or external breach. DHS stated that:

> We have…[an] internal protocol, where on identification of a threat or exposure, that information is raised by the chief information security officer to [the Chief Information Officer, who then briefs] the secretary. The secretary then has a subgroup of the executive part of the internal cyber group which assesses the implication of the threat and determines the actions and the additional officers that need to be brought in. In most recent cases, the view has been taken that external agencies like ASD will be informed of what we know at the time of the threat and, depending on the circumstances, we involve the AFP at early stages to make sure we have sufficient forensics and so they can have the best possible information to take it further, should they wish to.[75]

---

72 AGD, *Australian Government protective security governance guidelines – Reporting incidents and conducting security investigations*, 2011, p. 1.

73 AGD, *Australian Government protective security governance guidelines – Reporting incidents and conducting security investigations*, 2011, p. 7.

74 Major General Stephen Day, Deputy Director, Cyber and Information Security, ASD, *Committee Hansard*, Canberra, 24 October 2014, p. 15.

75 Mr Gary Sterrenberg, Chief Information Officer, DHS, *Committee Hansard*, Canberra, 24 October 2014, p. 16.

5.63 The ATO outlined its reporting policy and processes and highlighted its IT Security Incident Response program, stating that:

> All ATO IT Security incident reporting is cascaded to the key operational and security committees within the ATO for full transparency and oversight. Government policy requires the ATO to report significant breaches, which the ATO does mainly through close collaboration with the Australian Signals Directorate Cyber Securities Operations Centre. The ATO has a strong 24x7 IT Security Incident Response program, which consists of IT security incident reporting, response and monitoring, all supported by formal processes. These processes are clearly documented, embedded within mandatory organisational policy and cascaded throughout the ATO so that the required members of the critical response team can act effectively and efficiently. The ATO's Incident Response capability has been recognised with an award from the Australian IT Security response organisation AustCERT.[76]

5.64 Customs discussed its proactive Security Operations Centre, stating that:

> The Australian Customs and Border Protection Service (ACBPS) operates a proactive Security Operation Centre (SecopsCen) which utilises a range of specialist security tools integrated into a Security Information & Event Management (SIEM) system. This system is based on similar technology and processes used by the Australian Signals Directorate (ASD) Cyber Security Operations Centre (CSOC). In all cases the incident is advised to the ACBPS Strategic Border Command Centre who assesses the incident in the context of national border security operations. The ACBPS SecOpsCen is the single source of truth for all reported or detected security incidents, not just cyber incidents. The ACBPS has close collaboration with the ASD CSOC on matters that relate to vulnerabilities, threats, methods and practices. This close collaboration with ASD provides the ACBPS with expert guidance and or resources to assist with the matter.[77]

5.65 The Department of Defence (Defence) informed the Committee that all breaches are reported to the Defence Security Authority through a standard reporting process. Defence noted that the specifics of their reporting processes are sensitive but assured the Committee that they have dedicated teams of highly specialised, well trained operators who:

76 Australian Taxation Office (ATO), *Submission 9*, p. 1.

77 Australian Customs and Border Protection Service (Customs), *Supplementary Submission 5.1*, p. 1.

monitor Defence's cyber environment; conduct vulnerability scanning and assessments; and provide advice and assistance to their capability delivery areas 'to ensure that security is an essential element of everything we do.'[78]

Committee comment

5.66 The Committee is keenly aware of the importance of ensuring that the ICT systems of Australian government agencies are adequately protected from both internal and external threats. The Committee is concerned that, of the seven agencies audited, not a single agency was found to be fully compliant with the top four mitigation strategies and related controls in the ISM at the time of audit and none of the agencies was expected to achieve full compliance by the mandated target date of July 2014.

5.67 The Committee acknowledges the comments from ASD and the selected agencies regarding the challenges that many agencies have faced and will continue to face when implementing these strategies. However, the Committee agrees with the ANAO's comments that:

> 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.[79]

5.68 As such, the Committee feels that agencies should be seeking to achieve full compliance as soon as possible, and have a clear and detailed plan providing a definitive date by which they will achieve compliance.

78 Department of Defence (Defence), *Submission 7*, p. 1.

79 ANAO, Audit Report No. 50 (2013-14), p. 57.

Recommendation 8

5.69 **The Committee recommends that the seven agencies audited by the ANAO achieve full compliance with the top four mitigation strategies and related controls in the Information Security Manual as soon as possible. Further:**

- **each agency should produce a clear and detailed plan of necessary activities, including a definitive date of compliance**
- **agencies that do not expect to achieve full compliance before August 2015 should notify the Committee – the Committee may then seek an explanation of why full compliance is not expected to be achieved, as well as the mitigation strategies the agency has put in place**

5.70 The Committee commends the ANAO for its audit of the selected agencies' ICT systems and its considered approach to reporting its findings. In particular, the Committee points to the ANAO's follow up with each selected agency, which included a detailed issues paper, addressing specific findings for each agency. The Committee further commends the ANAO for providing detailed and tailored briefings and presentations regarding the general and specific findings of the report to agencies' senior executives and ICT officers.[80]

5.71 The Committee notes Major General Day's comments that 'one of the problems we have at the moment is whether people are actually aware that there is a threat, let alone knowing what to do about it and then actually doing something about it…it is not just about technology; it is also about people.'[81] The Committee believes that the ANAO's audit has assisted agencies to understand the vulnerabilities of their ICT systems and the ways in which they can improve the security of their systems.

80 IP Australia, *Submission 6*, p. 2.

81 Major General Stephen Day, Deputy Director, Cyber and Information Security, ASD, *Committee Hansard*, Canberra, 24 October 2014, p. 15.

Recommendation 9

5.72 **The Committee recommends that the Australian National Audit Office consider including regular audits, in its schedule of performance audits, of Commonwealth agencies' compliance with the top four mitigation strategies and related controls in the Information Security Manual as well as Commonwealth agencies' overall security posture.**

5.73 The Committee supports the CSOC and its work providing personal assistance and tailored advice to agencies as they improve the security of their ICT systems. The Committee commends the collaborative nature of the CSOC and its pooling of the cybersecurity capabilities of ASD, the Cyber Espionage Branch of ASIO, the Computer Emergency Response Team from the Attorney-General's Department, the Australian Federal Police and Australian Crime Commission.

5.74 The Committee encourages all Commonwealth agencies to work closely with the CSOC to ensure that their ICT systems are adequately protected from internal and external threat and all breaches are reported and addressed without delay.