Australian Government

Department of Immigration and Border Protection

Inquiry into Cybersecurity Compliance

Joint Committee of Public Accounts and Audit (JCPAA)

Table of Contents

Introduction....3

DIBP Submission....4

Progress table....7

Introduction

The Department of Immigration and Border Protection (the Department) recognises that robust, secure systems are a vital component to good government. The Department appreciates the work of the Australian National Audit Office (ANAO) in identifying areas for improvement.

The Department recognises that targeted cyber intrusions remain the biggest threat to government ICT systems. Compliance with the Top Four mitigation strategies helps protect an organisation from low to moderately sophisticated intrusion attempts and makes it significantly more difficult for an adversary to run malicious code on ICT systems.

The Department agrees with the findings of the report and supports the recommendations.

However, in considering the findings raised in the report, it is important to recognise the previous audit tabled in June 2014, ANAO Audit Report No. 50 2013-14, *Cyber Attacks: Securing Agencies' ICT Systems*, which assessed the former Australian Customs and Border Protection Service (ACBPS). The current audit assessed the Department of Immigration and Border Protection, which operates in a significantly more complex environment, from migration policy, visa and cargo processing to frontline border operations involving the timely movement of people and goods across the border that includes civil maritime security operations and border law enforcement activities.

July 2015 saw the disestablishment of the ACBPS and the creation of the Australian Border Force as part of an integrated immigration and border protection portfolio. From an ICT perspective, this presented an enormous challenge of integrating two very different ICT architectures, ICT operational management processes and cybersecurity maturity. Combined, the two agencies have over 900 applications, of which 569 are unique. Of the 279 business critical applications, approximately 70% are bespoke.

These applications are supported by over $250 million of ICT infrastructure that is located in 84 regional locations around Australia and 51 offshore posts. The integrated portfolio had multiple external service providers including two telecommunications and two mainframe processing providers, which have now been transitioned to single providers.

Both the Department of Human Services (DHS) and the Australian Taxation Office (ATO) have invested heavily over the last three to five years in large cybersecurity and ICT investment programmes. The Department of Immigration and Border Protection, however, is only in its second year of a number of multi-year programmes - Security; Identity and Access Management; End User Computing Consolidation and ICT Consolidation - that will significantly enhance the Department's cybersecurity capability.

The Security Programme includes a dedicated project focused on delivering and maintaining compliance with the ISM Top Four mitigation strategies. This project will deliver this financial year:

- Improved and effective application whitelisting across all desktops by July 2017.
- Improved cybersecurity compliance and vulnerability reporting to the Department's Executive.

The Identity and Access Management (IAM) Programme incorporates significant improvements in the overall management of privileged accounts including a proof of concept for the introduction of multifactor authentication for privileged accounts to be completed this financial year.

The End User Computing Consolidation (EUCC) Programme, due to be completed by June 2020, will introduce a single departmental end user ICT environment BorderNet (this includes a single desktop, printing service, email and file systems). It is complementary to IAM and Security programmes as it will deliver more robust ICT security controls including improved user account management, application whitelisting and security auditing are built into BorderNet. The EUCC

programme has already commenced rolling out the new desktop, which includes application whitelisting.

The move to a single departmental ICT environment, that will include the rationalisation of the Department's large application and infrastructure environment, is also progressing and is due to be completed by 2020. The cost of these integration initiatives have been absorbed by the internal departmental budget.

The risks associated with the compromise of the Department's key ICT systems are clearly understood by the Department and are articulated in the Department's Enterprise Risks.

While acknowledging the shortcomings identified by the ANAO report, the Department has security controls in place with no reported successful attacks on the Department's ICT systems.

The Department is committed to protecting information holdings from threat and continues to build cyber security resilience and embraces the concept of Defence in Depth. The Department has identified a number of controls to mitigate the risk of targeted cyber intrusions, including compliance with the Top Four mitigation strategies, including:

1. Establishing accredited secure gateway environments to mitigate targeted cyber intrusions by enforcing a range of layered security controls.
2. Deployment of endpoint protection to servers and workstations to detect malware and indicators of compromise.
3. Monitoring and alerting of security events is undertaken by a dedicated cyber operations function.

The following information submitted to the Inquiry relates to the current status of implementation against the audit recommendations, and future plans and milestones.

DIBP Submission

The Department has considered the recommendations made for all agencies in scope of the audit, as well as the findings particular to the Department. A table of actions taken to date is attached to this submission.

The Department is working towards full compliance with ASD requirements through a number of activities including:

a. Governance and Assurance

   i. The role of Chief Information Security Officer (CISO) has been elevated to the First Assistant Secretary of the ISA Division which satisfies the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) requirements that a Senior Executive position be responsible in this role.

   ii. The Audit and Assurance Branch, as part of its rolling strategic assurance program for 2017-2018, will include a review of cybersecurity executive oversight and governance.

b. Application Whitelisting Controls

   i. The ISA and ICT Divisions have in flight projects that will deliver improved and effective application whitelisting controls.

   ii. The EUCC is currently deploying the new Windows 10 desktop that is compliant with application whitelisting.

   iii. A strengthened application whitelisting solution is being deployed to all legacy Windows 7 workstations and will be completed by July 2017.

iv. By July 2017, all legacy (Windows 7), new Windows 10 including corporate issued laptops and surface devices that connect to the internal network, will have application whitelisting enabled and enforced.

v. The Department is working towards delivering an application whitelisting capability to the Department's server fleet. This is a multi-year project and is expected to conclude by July 2018.

c. Patching of Operating Systems & Applications

i. There are significant challenges to the Department for regular patching of services and the broader maintenance of the Department's ICT systems, including disruption to business operations. However, it is acknowledged that security patching of ICT systems is one of the Department's core BAU activities that must be undertaken to protect ICT infrastructure and information from disruption or theft from external advanced persistent threats.

ii. The Department is developing a business case for the 2017/18 financial year to increase the patching frequency commencing to comply with the ISM requirements.

iii. The business case will be presented to the Department's Executive Committee for a strategic discussion and decision on options to enable a sustainable security patching regime.

iv. Improvements to security patching include:

1. The NPP funded Security Programme is delivering a capability to introduce real-time compliance and vulnerability reporting of server and workstations (and other ICT systems).

2. The capability will automate a number of assurance, compliance and reporting processes and will present a single source of truth of patching compliance across multiple environments and systems.

3. This reporting will be available for cyber assurance, ICT operations teams, governance boards (Vulnerability Management Board and Technology Enabling Programme Board) and the senior executive via a corporate dashboard.

d. The ANAO identified that the Department has configured its desktop application whitelisting policies to allow over 1400 users to by-pass the whitelisting controls through the use of lightly managed machines (users with workstation administrative privileges. The Department undertook a risk assessment at the time (March 2014) to consider the risk.

e. The issue at the time of the risk assessment related to the inability of the Department to deploy software applications (package applications) for developers and ICT support staff in a timely manner. As such there was a requirement for this cohort to have the ability to manage their own development and support applications.

f. The Department acknowledges that it does need to address its approach with lightly managed users and has been undertaking the following activities:

i. The EUCC has developed a Windows 10 Developer Desktop based on virtual desktop technology which will allow the removal of the lightly managed accounts from the production ICT environment.

ii. An audit and verification of lightly managed user accounts has been initiated with the aim of reducing the number of lightly managed in the interim until a new solution is available in mid-2017 that will negate the need to lightly manage accounts.

g. The Department has also implemented a number of additional controls to protect itself against intrusion. These include:

   i. Accredited secure gateway environments are in place to mitigate targeted cyber intrusions by enforcing a range of layered security controls.

   ii. Endpoint protection is deployed to servers and workstations to detect malware and indicators of compromise.

   iii. Monitoring and alerting of security events is undertaken by a dedicated cyber operations function.

In addition to the above cyber security initiatives, an Administrative Compliance Review, led by the Chief Operating Officer, will provide assurance to the Secretary and Commission that the Department is compliant with all applicable administrative requirements which arise at law, under regulation or pursuant to departmental policies, by 30 June 2017. The exception to this will be in cases where full compliance would be reliant upon major IT upgrades, with an interim compliance to be effected by 30 June 2017.

Progress table

DIBP ACTION AGAINST ANAO RECOMMENDATIONS AND FINDINGS

ANAO Cybersecurity Follow-up Audit

Type	ANAO Assessed Vulnerabilities	DIBP Response and Actions
Recommendation 1	Agencies should periodically assess their cybersecurity activities to provide assurance that they align with the Top Four mitigation strategies and the agencies' own ICT security objectives.	• The Department agreed with the recommendation and will assess its cyber security activities on an annual basis.
Recommendation 2	Agencies should improve their governance arrangements by: • asserting cybersecurity as a priority • ensuring appropriate executive oversight of cybersecurity • implementing a collective approach to cybersecurity risk management • conducting regular effectiveness reviews and assessments of their governance arrangements	• The Department agreed with this recommendation and has commenced actions to improve its governance arrangements for cybersecurity. • To improve executive oversight of cybersecurity, the Chief Information Security Officer (CISO) role has been elevated to the First Assistant Secretary Integrity, Security and Assurance position. • A review of cyber security executive oversight and governance is also planned for the Department's 2017-18 strategic assurance programme.
Finding	The Department was not meeting the requirements for application whitelisting on desktops and servers to prevent malicious software from running on a computer	• The Department has in flight projects that will deliver improved and effective application whitelisting controls. • By July 2017, all legacy (Windows 7), new (Windows 10) desktops, corporate issued laptops and surface devices that connect to the internal network, will have application whitelisting enabled and enforced.

Type	ANAO Assessed Vulnerabilities	DIBP Response and Actions
		• The Department is working towards delivering an application whitelisting capability to the Department's server fleet. Deployment is expected to be completed by July 2018. • The completion of these activities will provide full compliance with the ASD Top Four strategy – Application Whitelisting.
Finding	The Department was not applying adequate application and operating systems patching to protect systems from known vulnerabilities	• The Department is developing a business case for the 2017/18 financial year to increase the patching frequency. The business case will be presented to the Executive Committee for a strategic discussion and decision on options to enable a sustainable security patching regime. • The outcomes of the business case if approved will provide a significant improvement to the Department's patching regime. The Department will reassess its compliance with the ASD Top Four strategies for application and operating systems patching in December 2017.
Finding	The Department has insufficient protection against cyber-attacks from external sources	• There have been no reported successful attacks on the Department's ICT systems. A number of incidents have been prevented from escalating through the organisation by the security controls in place. The mitigating controls in place, which have proven to be effective include: - Accredited secure gateway environments are in place that mitigate targeted cyber intrusions by enforcing a range of layered security controls. ▪ The Gateway environments are reviewed by an ASD accredited assessor on an annual basis. ▪ Regular penetration test of the Gateway environments are undertaken. ▪ There is a funded project underway to enhance the Department's Distributed Denial of Service (DDOS) protection by July 2017.

Type	ANAO Assessed Vulnerabilities	DIBP Response and Actions
		- Endpoint protection is deployed to servers and workstations to detect malware and indicators of compromise. - Monitoring and alerting of security events are undertaken by a dedicated cyber operations function. • The Department also works closely with external partners such as the Australian Cyber Security Centre who bring together existing cyber security capabilities across Defence, the Attorney-General's Department, Australian Security Intelligence Organisation, Australian Federal Police and Australian Crime Commission in a single location.
Finding	ICT contracts did not align with the Top Four mitigation strategies, and service provider self-assessments were not being independently validated.	• The Department has now included a requirement for its major ICT service providers to undertake an annual ASD approved I-RAP assessment on the services provided. • The remediation activities from the I-RAP assessments will be closely monitored by the Department to ensure the service providers remediate any non-compliances with the Top Four mitigation strategies as soon as practicable.
Finding	The Department needs stronger monitoring, evaluation and review of Top Four compliance	• The role of Chief Information Security Officer has been elevated to the FAS Integrity, Security and Assurance position which satisfies the Protective Security Policy Framework and Information Security Manual requirements that a Senior Executive be responsible for this role. • The Department's Internal Audit function will deliver a detailed review and recommendations to strengthen cybersecurity executive oversight and governance by July 2017. Planning for the audit is currently underway.