Australian Government

# Australian Government response to the Joint Committee of Public Accounts and Audit Report: 467

# Cybersecurity Compliance

April 2019

The Australian Government would like to thank the Joint Committee of Public Accounts and Audit for the opportunity to respond to Report 467: *Cybersecurity Compliance.*

Protecting Australia from cyber threats is one of our greatest national security challenges. Malicious cyber activities have the potential to seriously harm our nation's security, stability and prosperity, as well as our federal agencies' ability to effectively serve the public and keep their trust.

Successfully meeting the challenges of digital transformation demands a different approach from Government. Traditional demarcations between policy and operations are no longer appropriate and geographic delineations are less relevant. That is why the Australian Government has taken decisive action to create a coordinated, Whole-of-Government cyber security capability, and why the Government's response to the Committee is a true coordinated Government position.

Rather than a traditional split between policy and administrative responses, the following submission represents a consolidated response from the Australian Signals Directorate, the Attorney-General's Department, the Australian Taxation Office, the Department of Home Affairs (formerly the Department of Immigration and Border Protection) and the Digital Transformation Agency. As the Government progresses the implementation of this response, we will continue to work in partnership across all levels of government, the private sector and the community to raise the collective level of cyber security and understanding of the risks facing all Australians.

The recent consolidation of policy and operational capability within the Department of Home Affairs and the Australian Cyber Security Centre (ACSC) respectively, has strengthened and streamlined the Government's ability to not only respond to cyber security incidents but become exemplars of cyber security best practice. To support entities, the Government, through the ACSC and the Department of Home Affairs, will take more proactive steps to partner with *Public Governance, Performance and Accountability Act 2013* entities to establish effective behaviours and lift their cyber security in ways that accurately address both the barriers they face and their unique risk environments.

The Government welcomes further opportunities to engage with the Committee on this matter.

# Contents

## Recommendation 1

The Committee recommends that the Australian Taxation Office and Department of Immigration and Border Protection report back to the Committee on their progress to achieving full compliance with the Top Four mitigation strategies by June 2018, including advice as to barriers and timelines to complete outstanding actions.

**The Australian Government agrees that the Australian Taxation Office (ATO) and Department of Home Affairs report back to the Committee on their progress to achieving full compliance with the Australian Signals Directorate's (ASD) Top Four Mitigation strategies.**

The ATO achieved compliance with the Top Four mandatory mitigation strategies for targeted cyber intrusions in November 2017, and is progressively implementing the ASD Essential Eight.

An independent review to provide assurance of the ATO's Top Four compliance and progress against the ANAO recommendations to ensure cyber security activities are aligned with the outcomes of the Top 4 is being conducted this financial year.

The Department of Home Affairs applies a defence in depth approach to cyber security which achieves a secure end state through application of practiced measures. This approach involves:

- an accredited and resilient secure gateway which manages any traffic into and out of the Department's corporate environment;
- layered technical controls that manage access to information and systems;
- regular penetration tests and vulnerability assessments of the Department's systems;
- rolling system assessments through the Department's security accreditation framework throughout their lifecycle; and
- governance controls including, policies and procedures, a Cyber Risk Management Board that oversights cyber security issues and regular internal and external reviews of the Department's cyber security capability.

These controls have been effective in preventing intrusions to departmental systems or the compromise of data. The Department is always looking to improve its cyber resilience and remains cognisant of the evolving threat environment, achieved in part through engagement with Australia's intelligence agencies.

The challenges to achieving compliance with the ASD Top Four mitigation strategies by June 2018 are a result of consolidating legacy ICT environments.

The Department of Home Affairs is now compliant with three of the Top Four mitigation strategies – application whitelisting, operating systems patching and restricting administrative privileges.

Notwithstanding the Department's 24 hour global operations which facilitate growing trade, migration and travel that feed Australia's economy, monthly application patching has commenced and a risk assessed approach is being taken to achieve technical compliance with the final control in the ASD Top Four by June 2020.

## Recommendation 2

The Committee recommends that the Australian Government mandate the Australian Signals Directorate's Essential Eight cybersecurity strategies for all *Public Governance, Performance and Accountability Act 2013* entities, by June 2018.

**The Australian Government notes the Committee's recommendation to mandate ASD's Essential Eight strategies to Mitigate Cyber Security Incidents, but agrees to extend cyber security controls to all PGPA Act entities.**

Mandating the Essential Eight

The Government is committed to ensuring all Commonwealth entities raise their level of cyber security and understand the risks they face. The Essential Eight represents ASD's best advice on the measures an entity can take to mitigate the threat of a cyber incident and manage their risks. However, the Government will consider mandating the Essential Eight when cyber security maturity has increased across entities.

The cyber security maturity and implementation of the Essential Eight strategies within entities is currently both a compliance and risk management issue for each accountable authority, due to the unique risk environments and operations of each entity.

To progress toward implementation of the Essential Eight, the Government will undertake the following actions to assist entities to improve their cyber security maturity:

- continuing to require compliance with four of the Essential Eight requirements;
- strongly recommending implementation of the other four Essential Eight strategies; and
- requiring reporting data on implementation of the Essential Eight as part of a new PSPF reporting maturity model.

To support entities, the Government, through the Australian Cyber Security Centre (ACSC), will take more proactive steps to partner with *Public Governance, Performance and Accountability Act 2013* (PGPA Act) entities to establish effective behaviours and lift their cyber security. Implementation of the Essential Eight will then be supported by the ACSC expanding its assistance and adopting a co-assurance posture. As noted in the response to ANAO Report No.53 2017–18 *Cyber Resilience* tabled on 28 June 2018, the Department of Home Affairs (Home Affairs), the Attorney-General's Department (AGD) and ASD will also work together to strengthen the standard of cyber security of Australian Government networks through enhanced technical guidance, improved verification and increased transparency and accountability.

Extension to all PGPA Act entities

The Australian Government agrees to pursue options to extend cyber security requirements to all Commonwealth entities under the PGPA Act.

As the PSPF is a government policy, section 21 of the PGPA Act requires non-corporate Commonwealth entities (NCCEs) to act in a manner that is 'not inconsistent' with the PSPF. As the PGPA Act does not require corporate Commonwealth entities (CCEs) to apply government policy generally, the PSPF currently only reflects better practice for CCEs.

A legislative obligation is necessary to extend cyber security requirements to CCEs. This could be achieved through legislative reform, for example to the PGPA Act framework, or through a government policy order under section 22 of the PGPA Act.

The Government will consider the implications of the PGPA Act 2013 and Rule Independent Review when considering options to extend cyber security obligations to CCEs. Timing for implementing this recommendation, including the most appropriate controls to mandate, will be guided by the best means of extending the obligation and consultation with affected entities.

## Recommendation 3

The Committee recommends that the Australian Taxation Office and Department of Immigration and Border Protection report back to the Committee on their progress in implementing ANAO Recommendation 1, including advice as to barriers and timelines to complete outstanding actions.

**The Australian Government agrees that the ATO and Department of Home Affairs report back to the Committee on their progress in implementing ANAO Recommendation 1.**

In relation to progressing ANAO Recommendation 1, the ATO has:

- implemented regular assessment of strategies and priorities relating to cyber security by the ATO Security Committee which has strategic responsibility for the ATO's security objectives;
- improved governance for security across the ATO with third party suppliers to monitor the level of compliance, a refreshed cyber security strategy, and program of work to ensure resilient, compliant systems that promote trust;
- introduced a multifaceted approach to cyber security to continuously strengthen the ATO's security posture that incorporates vulnerability management, regular security risk and threat assessments, strategy and policy, system certification reviews, and a monitoring and compliance regime; and
- strengthened contract clauses to more effectively ensure compliance.

In relation to progressing ANAO Recommendation 1, the Department of Home Affairs has:

- improved governance controls through the creation of the Cyber Risk Management Board that oversights cyber security issues with regular internal and external reviews of the Department's cyber security capability;
- created a dedicated Cyber Risk Services branch;
- established a defence in depth approach to cyber security; and
- is conducting an independent review of its cyber security capability.

## Recommendation 4

The Committee recommends that the Auditor-General consider conducting an audit of the effectiveness of the self-assessment and reporting regime under the Protected Security Policy Framework.

Response to this recommendation has been provided to the Committee separately due to the Auditor-General's independent status.

## Recommendation 5

The Committee recommends that the Attorney-General's Department and the Australian Signals Directorate report annually on the Commonwealth's cybersecurity posture to the Parliament, such as through the Parliamentary Joint Committee on Intelligence and Security.

**The Australian Government agrees that the Attorney-General's Department (AGD) and ASD, in consultation with the Department of Home Affairs will report annually on the Commonwealth's cyber security posture to the Parliament.**

The Australian Government agrees to provide an annual report on the Commonwealth's cyber security posture and will consider the appropriate conduit to the Parliament. The Government supports providing greater transparency in cyber security reporting and notes the new annual reporting process will provide an opportunity to streamline and enhance existing reporting processes.

The Government notes that neither AGD nor ASD have direct oversight of, or accountability for Commonwealth entities. Any report would be limited to information and obtained through survey instruments, cyber incident reporting and follow up investigations. Consistent with its responsibility for cyber security policy and coordination, Home Affairs will support AGD and ASD to drive improved standards of cyber security across Government, including though enhanced reporting to the Parliament.

## Recommendation 6

The Committee recommends that in future audits on cybersecurity compliance, the ANAO outline the behaviours and practices it would expect in a cyber resilient entity, and assess against these.

Response to this recommendation has been provided to the Committee separately due to the ANAO's independent status.

## Recommendation 7

The Committee recommends that the Australian Taxation Office and Department of Immigration and Border Protection report back to the Committee on their progress in implementing ANAO Recommendation 2, including advice as to barriers and timelines to complete outstanding actions.

**The Australian Government agrees that the ATO and Department of Home Affairs report back to the Committee on their progress in implementing ANAO Recommendation 2.**

In relation to progressing ANAO Recommendation 2, ATO has:

- featured cyber security as a priority in the ATO Corporate Plan;
- achieved compliance with the Protective Security Policy Framework, including compliance with the Top 4 cyber security mitigations is a formal performance measure in the ATO Corporate Plan, monitored by the ATO Executive Committee;
- directed the ATO Security Sub-Committee and Security Committee to monitor the implementation of the recommendations from the ANAO and other audits relating to cyber security;
- strengthened governance oversight through the ATO's Risk and Conformance Committee;
- increased governance oversight of third party supplier compliance through the ATO Operational Security Committee; and
- established a program of regular cyber security risk and threat assessments.

In relation to progressing ANAO Recommendation 2, the Department of Home Affairs has:

- restructured the Department's cyber security functions in September 2017, with the cyber security functions now organised under the ICT Division;
- established a dedicated Cyber Risk Services branch;
- created a Cyber Risk Management Board (CRMB) with SES representation from key areas across the Department to consider cyber risks, incidents and track compliance against the Top 4;
- regularly engaged external parties to review the Department's cyber governance arrangements; and
- conducted regular vulnerability assessments and penetration testing of high risk systems.

The Secretary of the Department of Home Affairs and the responsible Deputy Secretary of the Intelligence and Capability Group continue to focus on the outcomes of the audits and cyber security activities more broadly with regular briefings to stay informed of any cyber security incidents or threats.

## Recommendation 8

The Committee recommends that by June 2018, the Australian Government make the annual ASD survey mandatory for all *Public Governance, Performance and Accountability Act 2013* entities to complete.

**The Australian Government agrees to make the annual ASD survey mandatory for all NCCEs.**

Extension to all PGPA Act entities will be implemented in the context of considering options for extending PSPF reporting obligations to all CCEs, as set out in response to Recommendation 2.

In light of recent machinery of Government changes affecting Australia's cyber security governance architecture, the Government will review the various cyber security surveys issued to entities to reduce duplication and ensure the information collected is both applicable to all agencies and informs the Government's understanding of its cyber security posture. The Government will also consider this recommendation with reference to its response to the ANAO Report No.53 2017-18 Cyber Resilience tabled on 28 June 2018 and agreement by Home Affairs to work with AGD and ASD to explore options for developing a fit-for-purpose mechanism for verifying entities reported compliance.

## Recommendation 9

The Committee recommends the Australian Government make the Internet Gateway Reduction Program mandatory for all *Public Governance, Performance and Accountability Act 2013* entities.

**The Australian Government agrees to mandate a core Internet Gateway Reduction Program requirement for all PGPA Act entities as advised in Recommendation 1 of the *Review of Australian Government Internet Gateway Reduction Program*.**

Further detail on how this will be implemented will be considered as part of the Government's plan to pursue options to extend cyber security requirements to all Commonwealth entities under the PGPA Act as set out in Recommendation 2 and consideration of the remaining *Review of Australian Government Internet Gateway Reduction Program* recommendations.

Recommendation 10

The Committee recommends that the Digital Transformation Agency report back to the Committee on the review of the Internet Gateway Reduction Program, including:

- a progress report on the review by December 2017
- outcomes of the review and associated key actions and corresponding timelines by April 2018.

The Digital Transformation Agency has completed the requested review. A copy is included at Attachment A for the Committee's consideration.