Australian Government
Department of Human Services

AUSTRALIAN GOVERNMENT
DEPARTMENT OF HUMAN SERVICES

NEW JCPAA INQUIRY INTO CYBERSECURITY COMPLIANCE

SUBMISSION TO THE JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Table of Contents

Executive Summary

Cybersecurity is one of the Australian Government's highest priorities. The Department of Human Services (the department) has made a significant investment in this area aligned with Whole of Government policies and directives.

The Australian National Audit Office (ANAO) initially audited seven departments' compliance with the Australian Signals Directorate (ASD) mandatory Top Four mitigations as part of their performance audit *Cyber Attacks: Security Agencies IT Systems*, No. 50, 2013-14. This report assessed the Department of Human Services (the department) as having adequate process maturity and inadequate compliance.

In December 2015, the department developed and embarked on a three year program of work to strengthen and enhance its cyber security capabilities. The program was developed through extensive industry research, as well as the use of internal and external consultation and incorporation of the relevant frameworks and standards. The identified deliverables not only supported the government's agenda and the department's digital transformation, but ensured that the intent of the mandatory mitigation strategies were met.

A deliverable implemented by this program was a state of the art Cyber Security Operations Centre which was commissioned in December 2016. The addition of the facility has not only allowed the department to perform monitoring, reporting and incident management on a 24/7 basis, but has also significantly broadened security intelligence capability and event analysis. This change and other technical advancements have greatly improved the department's Cyber Security capability and posture.

Following the opening of the Cyber Security Operations Centre, in March 2017 the ANAO released the results of its Cyber Security Follow-up Audit. The results of this audit confirmed that the department was now considered "Cyber Resilient" and compliant with the ASD Top Four mitigation strategies. This confirmation demonstrates that the department is capable of continuing to provide services while deterring and responding to cyber attacks.

The report provided by the audit included two recommendations. The department agreed both recommendations and recognises these recommendations require ongoing focus and attention.

Part One – Response to Recommendations

These recommendations are not tasks that can be closed by a single ICT action, but rather require ongoing consideration to ensure they remain a part of business as usual processes and practices.

Recommendation One

- *The ANAO recommends that entities periodically assess their cybersecurity activities to provide assurance that:*
  - *they are accurately aligned with the outcomes of the Top Four mitigation strategies and entities' own ICT security objectives; and that they can report on them accurately. This applies regardless of whether cybersecurity activities are insourced or outsourced.*

Status Update:

The department recognises that its cyber secure and resilient status can only be maintained through regular review and mitigative actions.

The department has numerous Boards and Committees to which compliance with the Top Four mitigation strategies is reported. These all have senior executive membership and cross both the CIO Group and business areas. These include the Cyber Security Program Board, the ICT Compliance Board, the Security Steering Group and the Risk, Business Continuity and Security Committee. These forums all meet on a monthly basis and review compliance information that ensures the department remains compliant.

Recommendation Two

- *The ANAO recommends that entities improve their governance arrangements, by:*
  (a) asserting cybersecurity as a priority within the context of their entity-wide strategic objective;
  (b) ensuring appropriate executive oversight of cybersecurity;
  (c) implementing a collective approach to cybersecurity risk management; and
  (d) conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness.

Status Update

The department's governance structure incorporates cybersecurity at the foundations, ensuring oversight is enabled at operational and strategic levels.

The department's Chief Information Security Officer participates in the department's ICT Committee on a quarterly basis to provide updates on cybersecurity. The ICT Committee is comprised of the department's most senior executives and is chaired by the Secretary. It provides high level strategic and operational oversight relating to ICT issues across the department.

Part Two – Other Related Matters

In addition to the activities recommended through the audit, the department is undertaking the following initiatives.

- Active engagement with the broader cyber community, including participation in forums with other Chief Information Security Officers, both from the public and private sectors.
- The Cyber Security Branch is building learning capabilities and networks to not only meet its internal needs, but also to support the future needs of the wider community. This includes:
    - partnerships with other departments to facilitate staff exchanges, to assist in alleviating industry wide skills shortages
    - Cyber Wargames initiatives, providing the opportunity to share cyber skills and knowledge across government departments
    - a partnership with UNSW/ADFA to provide staff with targeted military grade instruction in cyber operations and tradecraft
    - the establishment of a training range to provide staff with practical experience in cyber events and scenarios
    - working with local educational institutions to provide students with information and work experience opportunities to foster career interest in cyber vocations
    - working with industry partners to implement best of breed technological capability.