Australian Government
Department of Defence

Office of the Secretary

R1-5-Secretary Suite
Russell Offices
CANBERRA ACT 2600
Telephone: 02 6265 2851

EC25-005756

EXECUTIVE MINUTE

on

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT REPORT 506: INQUIRY INTO COMMONWEALTH FINANCIAL STATEMENTS 2022-23

General Comments

1. In November 2024, the Joint Committee for Public Accounts and Audit ('the Committee') delivered its report on the inquiry into the Commonwealth's Financial Statements 2022–23. The inquiry was based on the Financial Statements 2022-23 audit report by the Australian National Audit Office (ANAO) which contained a Category A finding for Defence. The finding relates to 'unauthorised user access to Information Technology (IT) systems' from former Defence personnel and contractors.

2. Defence acknowledges and agrees the observations of the Committee in Report 506 regarding weaknesses in relation to the removal of access to IT systems for personnel and contractors who had ceased employment with the Department, contravening the requirements of the Protective Security Policy Framework and Information Security Manual.

3. Following the tabling of the ANAO report in 2024, Defence undertook a risk assessment and identified this as a systemic control deficiency, requiring a whole-of-Defence approach to address policy, process and tool weaknesses and oversight through the Defence Audit and Risk Committee (DARC).

4. To address this Category A finding, Defence completed the following actions to remediate the business risk identified:

a. Issued ICT Access Management Policy to reinforce obligations on Defence personnel;

b. Conducted a Defence-wide communication campaign on the mandatory use of Defence's online account management tool, to capture all users leaving Defence;

c. Updated the online account management tool workflow to improve the off boarding system process, by removing identified blockages and improving data sharing between Defence Groups;

d. Automated an account retirement system, removing access for users that hadn't off boarded through the online account management tool;

e. Implemented a detective control to identify potential users that retained access after leaving Defence, assess these users for high-risk access, and apply timely access removal treatment.

5. These efforts resulted in a significant reduction in instances of post separation access of Defence's network and systems and greater fidelity of separations data, allowing timely review and action of any off boarding deviations.

6. In February 2025, the ANAO acknowledged Defence's efforts and improvements during the 2023–24 Financial Statements audit review. The ANAO further recommended that Defence establishes assurance processes to regularly ensure the completeness and accuracy of terminations and network user account data and subsequently use role based positions to provide and monitor movement of access to IT systems, supporting user access processes and systems.

7. In addition to the immediate remediation activities, Project Trident was established in early 2025 to embed the ANAO's recommendations and enable both Defence and the ANAO to regularly test controls underpinning personnel separations as well as network and user access management data. Defence's Integrity and Assurance Division have provided independent oversight of Project Trident and undertook an internal audit of the project, providing a final audit report on 26 May 2025 to the DARC for consideration.

8. The Defence's Enterprise Resource Planning (ERP) foundational release (Tranche 1B) was implemented in May 2025, and is expected to support the ANAO's recommendation by providing better user access controls with the introduction of position based user roles within the Defence finance system. Position based user roles will continue to be implemented as ERP Tranches are released for additional functions.

9. Defence established the governance framework and assurance testing of repeatable and reportable data sets and engineered mechanisms that Defence and ANAO can test to ensure the completeness and accuracy of terminations and network user account data. A Defence internal audit has been initiated to provide an objective view of the effectiveness and completeness of actions taken.

10. As a result of the remediation efforts and the establishment of Project Trident, the ANAO concluded that the activities undertaken in 2024–25 materially addressed the risks outlined in the previous audit finding. These efforts led to the Category A finding being downgraded to a minor (Category C) finding on 29 May 2025.

Recommendation No: 5

11. The Committee recommends that the Australian Taxation Office, Department of Defence, National Archives of Australia and Services Australia each report to the Committee within six months

of this report on their progress in closing the significant breaches relating to their governance and control of IT systems.

Summary of response: Agreed

Supporting rationale: Supported

[redacted]

Greg Moriarty

Secretary

12 September 2025