Australian Government

Department of Employment and Workplace Relations

Our Ref: EC23-000701

Deputy Secretary
Deborah Jenkins

Mr Julian Hill MP
Chair
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600
jcpaa@aph.gov.au

Dear Mr Hill

Inquiry into Commonwealth Financial Statements 2021-22

The Department of Employment and Workplace Relations (DEWR) provides this submission to the Joint Committee of Public Accounts and Audit (JCPAA) to support its consideration of the Auditor-General Report Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2022 (Report 8/ 2022-23).

As noted by the Department of Education (Education) in its response to the Committee of 20 February 2023, a shared services arrangement exists between DEWR and Education, with DEWR providing ICT, property, and other services to Education.

In the ANAO report, the former Department of Education, Skills and Employment (DESE) received a moderate (B) category finding, Timely removal of user access on termination. DEWR delivers these services to Education. This submission focuses on actions implemented as part of DEWR's response to Report 8 2022-23.

The report noted the status of ANAO findings as follows:

Category	Closing position (2020–21)	New findings (2021–22)	Findings resolved (2021–22)	Closing position (2021–22)
Moderate (B)	–	1	–	1
Total	**–**	**1**	**–**	**1**

There was one new moderate audit finding in relation to user Access Controls (Terminated Users). Report extracts and subsequent actions follow.

Timely removal of user access on termination

The report noted the following.

The ANAO identified instances where users had accessed the department's systems after completion of their employment/contract. The ANAO noted that there were delays in completion of Exit Advice Notification which triggers a number of actions across the department, including the termination access to ICT networks and systems.

The department has implemented a standard operating procedure which reviews the separation process. In addition, the department has also commenced work on automating the separation process. The effectiveness of these processes will be assessed by the ANAO as part of 2022–23 financial statements audit.

DEWR response and actions taken

The department had a number of existing user access controls in place prior to this finding that are aligned to the Australian Government Information Security Manual. These include:
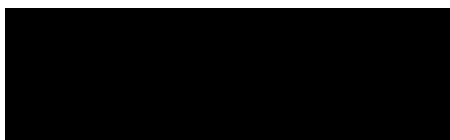
- The separating user or their manager is required to submit an Exit Advice Notification form in advance of their separation date.
- A twice daily synchronisation of SAP Human Resource (HR) record data and Microsoft Active Directory is undertaken.
- DEWR Information Communication Technology (ICT) network accounts for all types of contract or non-ongoing users are created only for the term of the user's engagement.
- Immediate removal of ICT access by end dating a user's Active Directory account on request by an authorised delegate in the event of any form of disciplinary action.
- Network accounts are automatically suspended after 45 days of inactivity, resulting in the user being unable to access the DEWR ICT network, the account is disabled after 90 days of inactivity.

As an interim response to the ANAO B finding, the DEWR Technology and Services Division has implemented an additional standard operating procedure (SOP) to review and validate all user separations for DEWR and Education. The SOP compares data extracted from 3 systems that are key to ICT network access controls and confirms that user separation dates are aligned in all 3 systems. Where any discrepancy is detected, the correct separation date for the user is investigated, confirmed, and updates are made, if required, to align systems. Up until early February 2023, no user separations have been identified that would require further examination.

DEWR has also implemented minor amendments to its Information Security Policy to allow staff to retain network access when on long term leave, secondment, or temp transfer in order to remain in contact with the department. Noting that if they don't access the network for 45 days their account is disabled in accordance with our standard controls.

The department is making a significant investment in a multi-year identity and access management (IAM) program of work. The IAM Program is currently in its second year and will modernise identity management, authentication, access controls, and privileged access management capability. It will deliver a definitive source of authority for IAM information, and automated checking and validation of user separations for the shared DEWR ICT network, as well as improved data quality.

Yours sincerely

Deborah Jenkins

28 March 2023