EXECUTIVE MINUTE

on

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT
REPORT No. 479
AUSTRALIAN GOVERNMENT SECURITY ARRANGEMENTS

General comments

The Joint Committee on Public Accounts and Audit (JCPAA) has requested the Department of Home Affairs (the Department) provide a response to recommendations 7-11 to its inquiry into Australian Government Security Arrangements based on the Australian National Audit Office (ANAO) Audit Report No. 43 2017-18, *Domestic Passenger Screening – Follow Up.*

The Department's responses to the recommendations are provided below. In summary, the Department has implemented a broad range of new initiatives that significantly improve the planning, monitoring and reporting of compliance and enforcement activities in the security regulated transport sectors.

Recommendation No. 7 paragraph 3.14

The Committee recommends that the Department of Home Affairs:

- *gather an appropriate baseline data set prior to the implementation of Regulatory Management System upgrade in the first quarter of 2019;*
- *monitor and review the outcomes of the upgrade against the baseline data set, particularly whether data quality is improving; and*
- *either prioritise an additional upgrade to the Regulatory Management System in order to establish an efficient and effective reporting function, or prioritise the development of the data product suite (as was approved on 10 November 2017) in order to address the limitations to data quality and performance reporting identified in the ANAO report.*

The Department supports this recommendation, has implemented a range of appropriate measures and considers it closed.

Since 2019 the Department has completed a number of initiatives that have resulted in multiple upgrades to the *Regulatory Management System* (RMS). These include mobile in-the-field capability, enhancements to regulatory assessments for entry control and the introduction of enforcement and infringement capability. These initiatives have introduced additional functionality

that automates and extends existing compliance business processes and significantly expands and improves the quality of datasets contained in the RMS.

The Department has also developed a new comprehensive data analysis and reporting capability in *Tableau* software which allows for more sophisticated analysis of compliance data that, in turn, better informs the targeting of compliance and enforcement activities. This capability also provides real-time analysis to the Department's regional compliance teams as they undertake audit, inspection and testing activities.

To specifically address the data limitations of the RMS, the Department has replaced a number of free text fields with drop down boxes and included new data fields to capture more detailed compliance information. This has resulted in improved consistency of data entry and therefore data analysis and reporting quality overall. The Department monitors RMS data standards.

Recommendation No. 8 paragraph 3.16

The Committee recommends that the Department of Home Affairs report back to the Committee on progress in the implementation of the compliance and enforcement framework in detail, including objectives, timeframes, milestones, lines of responsibility, performance measures, evaluation and reporting arrangements, and further information on the centralised case management system.

The Department supports this recommendation, has implemented appropriate measures and considers it closed.

Since the ANAO audit, the Department has introduced a new national compliance planning approach to ensure that compliance activity is focussed on the areas of highest security risk. A newly established function in the Department is responsible for security risk analysis as well as the planning and targeting of compliance activities and reporting on the National Compliance Plan's (NCP) effectiveness. Risk and compliance data as well as trends in findings are now continually assessed in order to refine targeting activity. The NCP is updated quarterly and is subject to on-going monthly reviews. Of note, all findings of non-compliance are followed up by subsequent compliance activity and, where required, enforcement action. The Department reports publicly on compliance activity as a key performance indicator in the Department's Portfolio Budget Statement. Internal reporting occurs weekly to senior executive in the Department.

The Department has also standardised its operational approach to the conduct and scheduling of audits, inspections and tests. This nationally consistent approach has resulted in improved data collection and data quality which, in turn, has enabled data benchmarking of like regulated entities and allowed for consistent comparative analysis of performance. Concurrently (and as stated in response to recommendation 7) the Department undertakes the analysis of RMS data using *Tableau* software. This capability improves the identification of non-compliance trends and security vulnerabilities and better informs compliance targeting.

The Department has also introduced screening performance standards for screening airports (see also Recommendation 11 below). These airports are now subject to a nationally consistent and

continuous passenger screening testing regime. The Department also works closely with the Australian Federal Police and international partners in the development and design of covert test weapons to ensure Australia's covert system testing is contemporary and effective.

The Department also provides screening airports with feedback on passenger screening performance, and chairs an industry working group to maximise the impact of the Department's system testing program. This working group discusses the development of test concepts and the results of system test activities. It also provides the opportunity for industry representatives to share with the Department (and each other) their initiatives aimed at ensuring a high standard of screening performance.

The Department published the *Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy* (the Strategy) on the Department's website in April 2022 to provide transparency to regulated entities on its approach to compliance and enforcement. The Strategy explains the key principles that underpin the Centre's regulatory, compliance and enforcement approach.

Recommendation No. 9 paragraph 3.18

The Committee recommends that the Department of Home Affairs report back to the Committee on training undertaken by staff in relation to the Regulatory Management System, and whether improvements to data quality, reliability and accuracy are being measured and achieved.

The Department supports this recommendation, has implemented appropriate measures and considers it closed.

The Department has observed significant improvements in the data quality, reliability and accuracy of the data in the RMS, which is linked to the reporting capability in Recommendation 7 above. Compliance officers now undertake mandatory online training in the use of the RMS. This training describes why and how the Department uses the RMS and explains the importance of good record keeping and data integrity. Training officers are embedded in all regional compliance offices. These officers both coach staff and monitor data quality and accuracy while new officers becomes familiar with the system. The Department's national compliance function regularly reviews the RMS compliance data records, and has observed improvements being achieved through a combination of controls, streamlined processes and the use of the *Tableau* reporting functionality.

In addition to online training, the Department has reviewed data entry fields to address relevant data capture. Quick reference guides have also been developed to assist compliance officers with the entry of compliance activities into the RMS.

Recommendation No. 10 paragraph 3.23

The Committee recommends that in relation to the learning and development framework, the Department of Home Affairs:

- *establish a formal monitoring mechanism to provide assurance that all ongoing and new operational staff have undertaken the required qualifications and re-accreditation; and*
- *consider using the results of the training needs analysis from February 2017 as baseline data in the monitoring and evaluation of the learning and development framework.*

The Department supports this recommendation, has implemented appropriate measures and considers it closed.

The Department remains focused on the training and development of its staff, and is continually assessing, monitoring and evaluating the training needs of its Aviation Security Inspectors (ASIs) and Maritime Security Inspectors (MSIs).

The Department utilised the 2017 training needs analysis as a baseline and has implemented online training solutions for ASIs and MSIs.

Currently to be considered for appointment as an ASI or MSI, candidates must:

1. complete four online training modules:
    - Induction Packages (including legislation training)
    - Introduction to the RMS
    - ASI and MSI Powers and Responsibilities in the Field, and
    - Regulatory Compliance Decision Making.
2. be enrolled in, or have completed a formal qualification to a minimum Certificate IV level in Government Investigations (or equivalent). Where the candidate is enrolled but has not yet completed a qualification, it must be completed within 12 months from appointment.
3. complete the relevant system test training module before they undertake a system test.
    - As the training module includes participation in a live system test, a candidate must be appointed as an ASI and have an ASI identity card issued to them before they can undertake the practical components of systems test training.

In conjunction with the formal training requirements, officers participate in practical regulatory activities alongside more experienced staff in order to consolidate their learning.

Instruments of appointment for an ASI and MSI now state that the appointment ceases after three years, or when they leave the Cyber and Infrastructure Security Centre (a Division within the Department responsible for regulatory compliance in the aviation and maritime sectors) whichever is the earlier. To be reappointed, an ASI or MSI must provide evidence that they have completed a refresher of the four online training modules.

Recommendation No. 11 paragraph 3.25

The Committee recommends that the Department of Home Affairs report back to the Committee on the implementation of performance measures for passenger screening, including:

- *the outcomes of the trial implementation period of performance measures with industry participants; and*
- *the department's target date for full implementation of performance measures.*

The Department supports this recommendation, has implemented appropriate measures and considers it closed.

As a result of the trial, the *Aviation Transport Security Amendment (Screening Information) Regulations 2021* amended the *Aviation Transport Security Regulations 2005* to introduce measures that:

- require screening authorities to create and retain records relating to security screening measures in place at their screening points;
- provide the Secretary with the power to set performance measures or targets for screening measures by way of a notice given to the screening authority;
- provide a person who has been issued with a notice specifying performance measures or performance targets with the opportunity to have that decision reconsidered by the Secretary in the first instance and, if the Secretary affirms the decision, to have the decision reviewed by the Administrative Appeals Tribunal;
- prescribe penalties for non-compliance with record making and retention requirements or performance requirements or targets set out in a notice;
- prescribe statistical data and contextual information relating to security screening measures as ***aviation security information*** for subsection 111(1) of the *Aviation Transport Security Act 2004* (Aviation Act).

Since the ANAO audit and the JCPAA recommendations, the Department has undertaken numerous initiatives to uplift the performance of passenger screening in Australia.

On 1 July 2022 the Department implemented the Performance Scorecard Framework (the Framework). This established a transparent performance expectation between the Department and designated airports in regards to passenger screening, with a focus on driving continuous improvements in airport security systems and security culture. The Framework assesses a number of factors relevant to an airport's security performance, including:

- its passenger screening system test performance;
- security culture and maturity;
- the standard of security equipment used by an airport; and
- an airport's own internal security testing and compliance governance.

The Framework considers a broad range of factors to address all aspects that affect security, and encourages airports to implement and demonstrate positive security behaviours and actions across the whole of their business.

The Framework allows for regular and consistent assessment of an airport's performance and allows for a comparison of airport performance across the network. The Framework also supports the assessment of an airport's performance over time in a consistent way, and allows for trends to be identified and addressed where appropriate.

As a result of the Framework's implementation, the Department has observed an uplift in industry's self-testing programs and investment in screening, including more active oversight of their performance. From 1 February 2023 the Framework was extended to other screened airports categorised as Tier One and Tier Two.

The Department has also introduced the Screener Accreditation Scheme through the *Aviation Transport Security (Screener Officer Requirements) Determination 2023*. The Scheme implements annual accreditation testing for all screening officers to ensure their ability to perform any screening functions under the requirements of the Aviation Act, associated regulations and relevant Aviation Security Notices.

Signed by
Hamish Hansford
Deputy Secretary Cyber and Infrastructure Security
Department of Home Affairs