EXECUTIVE MINUTE

on

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT
REPORT No. 479

Australian Government Security Arrangements

Summary

Defence agrees with qualification to Recommendation 3 directed towards it by Report 479. Timings of the implementation of the ICT 2270 Vetting Transformation project is subject to Defence project governance review and Government approval.

Defence agrees with Recommendation 4 of the report. Over the last 12 months Defence has put in place a number of additional measures to strengthen security around vetting information as part of wider Defence reform to enhance Defence Industry Security Program (DISP) requirements. The Australian Government Security Vetting Agency (AGSVA) is prioritising resourcing focused on external service provider Information and Communications Technology (ICT) security assurance.

Defence does not agree with Recommendation 5 of the report. The service delivery model for security clearances has been reviewed extensively in the last decade and is subject to a range of reform and review activities that are currently underway.

The strengthened personnel security reforms that were examined by the Australian National Audit Office (ANAO) report *Mitigating Insider Threats through Personnel Security (No. 38 2017-18)*, support future capabilities for sharing information across agencies to mitigate the insider threat. The reforms support future workforce growth and provide a mechanism to support a future workforce that will be adaptable and resilient, operating with greater flexibility and across organisational boundaries.

Defence continues to progress the two shared recommendations in the ANAO Report relating to the development of an enhanced risk information sharing framework with the Attorney-General's Department as a priority (Recommendations 1 and 3 of the ANAO report).

Implementation of these recommendations is still in progress. The framework was piloted between November 2018 and April 2019, and identified that further work was needed. There is a need to establish appropriate thresholds for what information is shared and ensure that entities have appropriate processes and governance arrangements for handling the sensitive personal information they receive. Further work is also required to support entities to have effective mechanisms to manage clearances that are subject to ongoing conditions.

The AGSVA Governance Board (a Deputy Secretary-level inter-agency board which meets quarterly) has considered the key findings of the Pilot and agreed to further test and refine the framework through a series of scenario workshops with an expanded field of participating entities, focusing on:

- further exploring what information is included in a protective recommendation, and how protective recommendations are handled by sponsoring entities,

- exploring complexities anticipated with conditional clearances including procedural fairness implications, and what expectations and resourcing are attached to managing conditional clearances, and
- clarifying what relevant 'information of security concern' should cover and therefore what information should be shared with sponsoring entities.

Advice on implementation will be provided to the AGSVA Governance Board and the Australian Government Security Committee by December 2019. It is anticipated that the recommendations will be completed by 31 March 2020.

The following is a response provided to each of the recommendations in Report 479 Australian Government Security Arrangements.

Response to the Report 479 Recommendations

Recommendation No. 3, paragraph 2.33

2.33 The Committee recommends that the Department of Defence expedite the ICT 2270 Vetting Transformation project and provide to the Committee a progress report and updated timeline on implementation of the replacement ICT system

Response: Agreed with qualification

Defence is managing the ICT 2270 Vetting Transformation Project to deliver a next-generation vetting system, in-line with industry capability, system requirements and acceptable risk levels.

ICT 2270 received National Security Committee (NSC) first-pass approval on 10 April 2018. Defence is scheduled to return to Government for second-pass consideration in quarter one 2020. To ensure the project is being effectively managed, in addition to normal Defence project management processes, the project is overseen by the inter-departmental AGSVA Governance Board.

Quarter one 2020 consideration allows for finalisation of outstanding procurement and risk reduction activities, robust overall cost assurance, and completion of initial system design.

Defence is currently undertaking cost and system design assurance activities following market engagement that commenced in October 2018. Based on this engagement Defence expects to engage the system integrator following NSC second pass consideration.

Additionally, as part of the broader vetting transformation project, Defence released requests for quote for a project delivery partner and organisational change management partner. These contracts are expected to be finalised following NSC consideration and will provide specialist expertise needed to assist in the management and delivery of the project.

Delivery of ICT 2270 is being managed in-line with delivery of a Defence wide Case Management System and updates to Defence's enterprise SAP systems. This is required to avoid duplication of basic case management tools across Defence, and ensure Defence systems can support full ICT 2270 functionality. This has resulted in a delay to the Interim Operating Capability, however no impact on the Final Operating Capability timeframe is anticipated.

Recommendation No. 4, paragraph 2.43

2.42 Despite this assurance,. the Committee is concerned that some vetting entities may have managers or company owners that are not Australian citizens who may have access to any some or all data handled by that entity.
2.43 The Committee recommends that the Department of Defence establish extra safeguards and quality control measures to ensure that no incidents of sensitive data loss occur prior to operational capability of the new vetting case management system.

Response: Agreed

Over the last 12 months Defence has put in place a number of additional measures to strengthen security around vetting information. In 2018, Defence completed a vetting system remediation program that enhanced ICT security controls. The eVetting system (PSAMS2) is now accredited against the Australian Government Information Security Manual.

In April 2019, Defence also strengthened DISP requirements, which all vetting providers must be members of. DISP members are required to apply Defence Security policies, including obtaining certification of physical premises and information systems, and personnel clearances for staff handling classified or sensitive information. All DISP members undergo Foreign Ownership Control and Influence (FOCI) checks and are required to provide reporting on security incidents and any FOCI changes.

DISP security requirements are reinforced by the recently established Defence Industry Security Office (DISO) which has responsibly for assuring DISP members' compliance. DISO conducts reviews and audits of DISP members (including Vetting industry members) to ensure appropriate security policies, systems and compliance regimes are in place.

In addition to the DISO assurance activities AGSVA is prioritising resourcing to increase External Security Vetting Service (ESVS) panel support staffing to create a new position focused on ESVS ICT security assurance.

AGSVA has undertaken a recent refresh of its ESVS panel, replacing the previous industry vetting panel. The new panel arrangements commenced on 12 August 2019 include increased security, professionalisation and capacity standards by requiring panel members to have a national vetting footprint and have all their vetting staff meet AGSVA-directed training competencies. These higher standards are expect to result in some consolidation of the smaller vetting providers, strengthening ESVS panel members' capability and proficiency.

Recommendation No. 5, paragraph 2.49

2.49 The Committee recommends that the Department of Defence prepare a full business case to consider the current and alternative service delivery models, taking account of projected future demand for vetting, the costs, benefits and risks of various approaches, and provide the findings of this to the Committee within 12 months.

Response: Not Agreed

The current whole-of-government clearance process and AGSVA has been reviewed extensively since AGSVA's establishment in 2010. Recommendations from the 2015 *Belcher*

Red Tape Review to reduce the regulatory burdens of the security vetting process were considered by Government in 2016 and resulted in a strengthened Commonwealth *Protective Security Policy Framework* from July 2018 and a comprehensively transformed security vetting process designed to mitigate the insider threats.

As a result of these reforms, the current clearance business model is delivering strong results in processing security clearances, while also providing the flexibility to meet future clearance demands. This strong performance has resulted in a reduction in all clearance timeframes and the elimination of Positive Vetting (PV) backlogs. Ongoing engagement and benchmarking with allies indicates that the reformed Australian vetting process is consistent with international best practice.

The External Security Vetting Service (ESVS) business model has been further strengthened by the August 2019 refresh of the Vetting Service provider panel. To meet projected vetting requirements, the new ESVS panel standards will raise panel members' security, capability and proficiency, as well as increasing overall panel vetting capacity.

Vetting clearance business processes will also be reviewed as part of the business process reform necessary to support the delivery of Vetting Transformation project ICT 2270. Defence is scheduled to return to Government for second-pass consideration in quarter one 2020. This formal project governance process will involve Defence Investment Committee and central agency review of the ICT 2270 project business case and capability requirements, including AGSVA organisational transformation, a future business operating model, and service delivery requirements.

Given the extensive range of reviews and reforms undertaken, and other reform activities still underway in relation to whole-of-Government vetting, a review in the next 12 months would not allow time for current and planned reviews and reforms to be completed, fully implemented and tested before drawing any conclusions or making further changes. Continuous business improvement is inbuilt into AGSVA's governance processes and service delivery. The evaluation of vetting reforms is also monitored through Defence project management processes, as well as being overseen by the interdepartmental Deputy Secretary-Level AGSVA Governance Board.

Greg Moriarty
Secretary
Department of Defence
23 August 2019

Angus J Campbell, AO, DSC
General
Chief of the Defence Force
23 August 2019