Australian Government
Attorney-General's Department

July 2019

Joint Committee of Public Accounts and Audit Report 479

Australian Government Security Arrangements

Attorney-General's Department Progress Report

Background

Following the release of the Australian National Audit Office (ANAO) report on *Mitigating Insider Threats through Personnel Security* (May 2018), the Joint Committee of Public Accounts and Audit (JCPAA) undertook an inquiry into Australian Government Security Arrangements, including implementation of the recommendations of that ANAO report.

On 2 April 2019, the JCPAA released its report, the *Inquiry into Australian Government Security Arrangements*. The JCPAA report made 11 recommendations, of which one is relevant to the department (Recommendation 2 of the JCPAA report).

Recommendation 2 is that the department provide the JCPAA with a progress report within three months and report to the JCPAA annually on implementation of the ANAO Report recommendations and the department's compliance with the Protective Security Policy Framework (PSPF).

The ANAO report made eight recommendations, six of which are relevant to the department (Recommendations 1, 3, 4, 6, 7 and 8). Of those, two recommendations are relevant to the department's policy role through the PSPF and support for the Australian Government Security Vetting Agency's (AGSVA) vetting services to effectively mitigate the insider threat by sharing information with entities of security concern identified in vetting processes or use clearance maintenance requirements effectively to minimise risk (Recommendations 1 and 3 of the ANAO Report). A further four recommendations are relevant to the department's own personnel security arrangements under the PSPF (Recommendations 4, 6, 7 and 8 of the ANAO Report).

This progress report includes a status update on the department's implementation of the ANAO Report recommendations.

Overview

The department has now fully implemented all four recommendations relating to its own personnel security (Recommendations 4, 6, 7 and 8 of the ANAO Report).

The department continues to work with Defence on the two shared recommendations in the ANAO Report relating to the development of an enhanced risk information sharing framework as a priority (Recommendations 1 and 3 of the ANAO report). Implementation of these recommendations is still in progress as a pilot conducted to test information sharing arrangements identified a range of complexities that need to be addressed to ensure appropriate mechanisms are in place for sharing sensitive personal information on potential security risks. The pilot, which concluded in April 2019, identified that further work needs to be done to establish appropriate thresholds for what information is shared by AGVSA and to ensure entities have effective arrangements for handling and using the information they receive. This is particularly important given the sensitivity of the personal information involved, including information about mental and physical health issues, personal relationships, drug and alcohol and financial issues. Further consideration is needed to support entities to have appropriate mechanisms in place to handle clearances which have ongoing conditions that need to be met for the purposes of maintaining an individual's clearance.

Below is an implementation status update, accompanied by information on future actions and changes made by the department in response to the audit's findings.

Implementation Status Update

Recommendation 1

The Department of Defence, in consultation with the Attorney-General's Department, establish operational guidelines for, and make appropriate risk-based use of, clearance maintenance requirements.	
Implementation Status	In progress – anticipated completion by 30 March 2020

The department continues to support AGSVA, in the Department of Defence, to implement this recommendation.

AGSVA, in consultation with the department and the Vetting Officers Community of Practice,[1] has amended its vetting risk model processes and documentation for vetting officers to support the use of clearance maintenance requirements. These documents will support AGSVA's vetting workforce to identify risks that can be mitigated by the application of specific clearance maintenance requirements and, where appropriate, to recommend that a delegate issue a clearance subject with a conditional clearance.

The operational guidelines have also informed AGSVA's implementation of the risk information sharing framework and were in tested in a pilot conducted by AGSVA (concluded in April 2019) as part of the response to Recommendation 3 below. The AGSVA Governance Board has considered the key findings of the pilot and agreed to undertake a series of additional scenario workshops to further test and validate the proposed framework, including the proposed operational guidelines.

This work complements the changes made in October 2018, as part of the reforms to the PSPF, to provide further guidance in the PSPF on the recommended process for granting a conditional clearance and responsibilities of sponsoring entities and authorised vetting agencies for the ongoing implementation of these clearance maintenance requirements. The reforms also clarified guidance on the existing obligations to share information about personnel security risk between authorised vetting agencies and sponsoring entities, to inform the application of the clearance maintenance provisions.

[1] The Vetting Officers Community of Practice is chaired by the department and all authorised vetting agencies are members. For further information, see Annex A.

Recommendation 3

The Attorney-General's Department and the Department of Defence establish a framework to facilitate the Australian Government Security Vetting Agency providing sponsoring entities with specific information on security concerns and mitigating factors identified through the vetting process.	
Implementation Status	In progress – anticipated completion by 30 March 2020

The department and AGSVA have developed a risk information sharing framework to facilitate sharing of specific information of security concern and mitigating factors identified through the vetting process, including where AGSVA determines the need to grant a conditional clearance.

The framework was tested in a pilot conducted by AGSVA, with support from the department, the Department of Home Affairs and the Australian Taxation Office, from November 2018 to April 2019. The pilot covered all levels of security clearances from Baseline through to Positive Vetting. Risk advisory notices were used to share information relating to security risks and mitigations, and to assist sponsoring entities in understanding the nature of risks and mitigations identified in the vetting process. The pilot highlighted that there is a need to further consider the best approach to share information of security concern while ensuring appropriate mechanisms are in place for handling sensitive personal information.

The AGSVA Governance Board has considered the key findings of the pilot and agreed to undertake a series of additional scenario workshops to further test and validate the proposed framework before advice on implementation is provided to the AGSVA Governance Board and the Australian Government Security Committee by December 2019.

The workshops will:

- further explore what information is included in a protective recommendation, and how protective recommendations are handled by sponsoring entities
- explore complexities anticipated with conditional clearances including procedural fairness implications, and what expectations and resourcing are attached to managing conditional clearances, and
- clarify what relevant 'information of security concern' should cover and therefore what information should be shared with sponsoring entities.

The department has developed draft guidance materials to support implementation of the risk framework (Recommendation 1 refers). These outline information management and handling to ensure there is a common understanding about how information can be shared with and between sponsoring entities and authorised vetting agencies, along with procedural fairness. The workshops will enable further testing of the operational guidelines.

Recommendation 4

The Attorney-General's Department conduct a personnel security risk assessment that considers whether changes are needed to their protective security practices.	
Implementation Status	Complete

The personnel and physical risk assessment of all the department's sites, including the Australian Government Solicitor offices nationwide, has been completed.

The department acknowledges the required two-yearly risk assessment was due to be completed by July 2017. This was delayed for a number of reasons, including the Machinery of Government changes announced in July 2017 and the subsequent reduction in responsibilities for national security and cyber security in the department over the period December 2017 to July 2018.

In 2018, the department engaged Forcefield Services, a SCEC Approved Security Consultant, to undertake the review. Forcefield Services provided the final risk assessment report in June 2019.

The department has commenced consideration of the findings and recommendations, and will implement additional security mitigation strategies identified as necessary and appropriate to meet our obligations under the PSPF and to protect our people, information and assets.

The report contains sensitive and security classified information including information about identified security vulnerabilities. If disclosed, that information could be exploited to the detriment of departmental personnel, information or assets. Accordingly, access to the report will be limited to departmental officers with a legitimate need to know.

Recommendation 6

The Attorney-General's Department implement quality assurance mechanisms to reconcile their personnel records with AGSVA's clearance holder records, and commence clearance processes for any personnel who do not hold a required clearance.	
Implementation Status	Complete

The department completed an audit of clearance holdings in March 2018 and reconciliation of the holdings was completed in September 2018.

During the reconciliation, the department identified 2560 inconsistencies. One significant reason for the inconsistency between our records and AGSVA records related to the Department of Communications and the Arts Machinery of Government change. AGSVA had been notified of the employees to be transferred however sponsorship was not transferred and those employees remained attached to the department's sponsorship. The department has rectified all inconsistencies.

The department will conduct an annual review of all its security clearance holdings by 31 December each year.

Recommendation 7

The Attorney-General's Department review their policies and procedures for eligibility waivers to ensure they are compliant with PSPF mandatory controls.	
Implementation Status	Complete

The department has reviewed its procedures for eligibility waivers to ensure compliance with the PSPF. The department does not have an agency specific policy concerning eligibility waivers as PERSEC 5 articulates all necessary aspects of the eligibility waivers policy.

The department has implemented an ICT upgrade to the database that stores information about eligibility waivers. This upgrade ensures the immediate assessment of any information relevant to the waiver and supports documented reviews of all waivers at the nominated review date. The ICT solution generates an automatic notification in advance of the nominated review date, which is the catalyst for the department to commence the review.

Recommendation 8

The Attorney-General's Department implement the PSPF requirement to undertake an annual health check for clearance holders and their managers.	
Implementation Status	Completed

In May 2019, the department implemented an annual health check process to support, assess and manage the ongoing suitability of security cleared personnel.

Implementation of the annual health check includes three main elements. A screensaver designed to remind departmental officers of the importance of discussing security issues with colleagues and managers, including as part of their regular performance discussions, is now in rotation on all departmental officers' computer screens. A Security Fact Sheet is now available as a supplement to the security information on the intranet. The Fact Sheet reminds staff of their security obligations, including the requirement to advise the Departmental Security Unit of changes in personal circumstances, travel and foreign contact of potential security concern. The Fact Sheet also reminds managers to discuss personnel security with staff during the final performance evaluation discussion will be available shortly. Information about security has been incorporated into the employee performance agreement template and guidance material for 2019-20, again reminding staff to engage proactively with security issues.

Future plans and milestones

Recommendations 1 and 3

The department and AGSVA have agreed on a combined and phased approach for implementing Recommendations 1 and 3 of the report.

Milestone action	Milestone date
Scenario workshops	September – October 2019
Provide a report to AGSVA Governance Board on the outcomes of these workshops, including any additional amendments to the Framework, and an implementation plan by December 2019 (including approach to consultation with GSC and Secretaries Board)	Report by December 2019
Full implementation of the information sharing framework (including operational guidelines)	by end March 2020

Annex A

Communities of Practice

Vetting Officers Community of Practice

The Vetting Officers Community of Practice comprises experienced Australian Government vetting officers and policy officers with responsibility for security vetting. This community of practice regularly meets to identify and refine best practices by vetting officers, develop tools and strategies to enhance the quality and consistency of vetting decisions, and promote information sharing, shared problem solving and horizon-scanning. The department coordinates and provides secretariat support for the Community of Practice.

Members of the Vetting Officers Community of Practice include all authorised vetting agencies, specifically:

- the Australian Government Security Vetting Agency in the Department of Defence
- the Australian Federal Police
- the Australian Security Investments Commission
- the Australian Security Intelligence Organisation
- the Australian Secret Intelligence Service
- the Department of Foreign Affairs and Trade
- the Office of National Intelligence

Non-vetting agency members include:

- the Department of Prime Minister and Cabinet
- the Department of Home Affairs
- the Australian Taxation Office
- the Australian Transaction Reports and Analysis Centre.