Australian National Audit Office

Joint Committee of Public Accounts and Audit

Mitigating Insider Threats through Personnel Security (Auditor-General Report No.38 of 2017–18)

17 August 2018

Opening Statement by Mr Grant Hehir, Auditor-General for Australia

1. Good morning Chair and committee members.
2. Thank you for the opportunity to appear before the committee today.
3. I am pleased that the committee has chosen to undertake this inquiry which highlights the importance of following up on previous audit recommendations. Follow-up audits are an important part of ANAO's work, holding entities to account and highlighting whether entities are responding appropriately to audit findings, particularly in terms of changing behaviours and processes.
4. Personnel security is a core component of the Australian Government's Protective Security Policy Framework (or PSPF). Effective personnel security arrangements underpin the protection of the government's people, information and assets by providing a level of assurance as to the eligibility and suitability of individuals accessing government resources. A previous audit (ANAO Report No.45 of 2014–15, Central Administration of Security Vetting), had identified deficiencies in Australian Government Security Vetting Agency's (AGSVA's) performance, which were of a nature that warranted a follow up audit.
5. The Australian Government Security Vetting Agency (or AGSVA), which is part of the Department of Defence, provides centralised security vetting services for most government entities. Government entities also have personnel security requirements under the PSPF to undertake employment screening of personnel, manage ongoing suitability, and share relevant information with AGSVA.

6. The objective of the 2018 Mitigating Insider Threats through Personnel Security audit was to assess the effectiveness of the government's personnel security arrangements for mitigating insider threats by considering whether: AGSVA was providing effective security vetting services; and selected entities were complying with PSPF personnel security requirements.

7. The entities selected for the PSPF compliance assessment were the Attorney-General's Department, Australian Radiation Protection and Nuclear Safety Authority, Australian Securities and Investments Commission, Department of Home Affairs and Digital Transformation Agency.

8. The audit found the effectiveness of the Australian Government's personnel security arrangements for mitigating insider threats is reduced by: AGSVA not implementing the Government's policy direction to share information with client entities on identified personnel security risks; and selected entities not complying with certain mandatory PSPF controls.

9. When AGSVA identifies security concerns during its vetting process it can either: accept the risk by issuing a clearance; reject the risk by denying a clearance; or mitigate the risk by granting a lower level clearance, imposing clearance maintenance conditions (such as regular drug testing), or communicating security concerns to an individual's sponsoring entity.

10. ANAO analysis found AGSVA often identified security concerns, but very rarely denied a clearance or used the risk mitigation options available to it. In addition, AGSVA had not met the intent of government's 2014 policy reforms to increase information sharing between with sponsoring entities, as it did not gain explicit informed consent to share information from clearance subjects.

11. The report made three recommendations regarding this, aimed at ensuring AGSVA: finishes updates to clearance holder consent requirements; and develops frameworks and guidelines, in consultation with the Attorney-General's Department, to make greater risk-based use of clearance maintenance requirements and provide risk information to sponsoring entities.

12. With regard to the cross-entity PSPF compliance assessment, our analysis found all entities were non-compliant with certain mandatory PSPF personnel security controls. Two entities had not undertaken personnel security risks assessments. One entity had not finalised a protective security plan and policies and procedures. Four entities did not have adequate controls and quality assurance mechanisms for ensuring personnel have appropriate clearances. Four entities had not fully comply with PSPF controls for eligibility waivers. None of the five entities were compliant with the requirement to undertake an annual health check.

13. The report made five recommendations relating to entity compliance, aimed at ensuring entities: have appropriate risk-based personnel security practices; implement quality assurance

mechanisms to reconcile their personnel records with AGSVA's clearance holder records; comply with eligibility waiver requirements; and undertake an annual health check process.

14. We would be happy to answer any questions the Committee may have.