



Level 5, 100 Market Street,
Sydney NSW 2000
GPO Box 9827, Sydney NSW 2001
DX 653 Sydney

Telephone: +61 1300 935 075

Facsimile: +61 1300 729 000

www.asic.gov.au

Our Reference: CCU-18\0317
Your Reference:

26 July 2018

Ms Susan Cardell
Committee Secretary
Joint Committee of Public Accounts and Audit
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Ms Cardell

Re: New inquiry into Australian Government Security Arrangements: Audit Report No. 38 (2017-18) *Mitigating Insider Threats through Personnel Security*

Public hearing and submission invite

Further to your letter of 3 July 2018 to James Shipton, Chair, Australian Securities and Investments Commission (ASIC), this letter provides an update on the implementation status and other activity relevant to the audit recommendations directed at ASIC arising from the *Mitigating Insider Threats through Personnel Security* Report.

Three of the eight audit recommendations were directed at ASIC:

1. Recommendation No. 6 – *ASIC implement quality assurance mechanisms to reconcile their personnel records with AGSVA's clearance holder records and commence processes for any personnel who do not hold a required clearance.*
2. Recommendation No. 7 – *ASIC review their policies and procedures for eligibility waivers to ensure they are compliant with PSPF mandatory controls.*
3. Recommendation No. 8 – *ASIC implement the PSPF requirement to undertake an annual health check for clearance holders and their managers.*

In response to Recommendation No. 6, ASIC has taken, or is taking, the following action:

- During April and May 2018, ASIC reconciled the ASIC personnel database and the AGSVA dashboard to identify personnel with expired or no security clearances.
- A tool was developed to identify the required security clearance level by role. Work is taking place with People and Development and individual business unit managers to confirm and document the required security clearance levels for all roles within ASIC.
- Two hundred and eighty-three (283) personnel were identified as requiring security clearances. Eighty-nine (89) clearance requests have been initiated to date, and we anticipate all will have been initiated by 31 December 2018. This is in addition to initiating clearance requests for all incoming personnel over this period.
- During June 2018, Highly Protected security clearances held by 202 personnel and expiring in December 2018 were revalidated to the Baseline clearance level. A further 495 personnel holding Highly Protected clearances due to expire in 2019 and 2020 will be revalidated to the appropriate level during early 2019.
- Working with AGSVA, ASIC sponsorship has been removed from all personnel no longer employed by or engaged with ASIC.
- As a part of the assurance plan, ASIC now conducts quarterly security clearance audits of the personnel database and reconciles the result with AGSVA records.

In response to Recommendation No. 7, ASIC has taken, or is taking, the following action:

- ASIC has implemented a process for requesting an eligibility (citizenship) waiver that includes:
 - Requirements for hiring managers to consider applications from Australian citizens only, in the first round.
 - If no Australian citizen applied for the position, ASIC can then consider applications from permanent residence holders. If no successful candidate is found, then non-Australian citizens are considered.
 - A requirement for the hiring manager to provide a detailed business case justifying the need to employ a non-Australian citizen.
 - ASIC Security Services conducting a risk assessment on potential candidates.
 - The business case and risk assessment are reviewed and approved by the Agency Security Adviser and the Chief of Operations, as delegated by the ASIC Chair.

- ASIC submit the eligibility waiver form, together with the business case and risk assessment to AGSVA for approval, prior to seeking a security clearance and a provisional access request where required.
- ASIC engaged external consultants, *Ethos CRS*, to redraft our existing policies and the above process will be incorporated into the Personnel Security Policy.

In response to Recommendation No. 8, ASIC has taken, or is taking, the following action:

- The Annual Security Compliance requirement has been incorporated into ASIC's internal Risk and Disclosure management system, commencing from July 2018.
- Staff are also required to report changes to their personal circumstances as they occur, on an ongoing basis.
- The revised Personnel Security Policy will reflect this requirement.

ASIC welcomes the opportunity to attend the public hearing on Audit Report No. 38 (2017-18) to be held on 17 August 2018 at Parliament House, Canberra. Included with this letter are Hansard Witness Forms for ASIC's intended representatives at this public hearing.

Yours sincerely,

Carlos Iglesias
Chief of Operations