

Joint Committee of Public Accounts and Audit

Parliamentary inquiry – Auditor-General's reports 38 and 43 (2017-18) –
17 August 2018

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: JCPAA - Auditor General's reports 38 and 43 (2017-18) - 17 August 2018 - Q2
Positive Vetting service provider ICT compliance - Brodtmann

Question reference number: 2

Member: Ms Gai Brodtmann

Type of question: Written

Date set by the committee for the return of answer: 14 September 2018

Question:

Mr Fortune: We have a panel arrangement of service providers, about 22 providers, and, of those, about 14 doing positive vetting clearances. They range from small to medium-sized enterprises to sole traders.

Ms BRODTMANN: So there are 14 entities.

Mr Fortune: That do PV clearances, within that panel.

...

Ms BRODTMANN: Most government agencies are compliant with the essential eight. Are all these 14 compliant with the essential eight?

Mr Fortune: We are working with them to understand what their risks are. Where they're not compliant, there is a program of remediation to address that.

Ms BRODTMANN: Are the 14 compliant with the essential eight?

Mr Fortune: I would have to take that on notice.

Ms BRODTMANN: If you could—

Mr Fortune: I'm not an ICT security expert. But I can tell you is that we have a robust program of external review and auditing through our staff to look at their security and ICT systems and to ensure that their risks are being managed consistently with the requirements.

Ms BRODTMANN: Okay, I get that; it's a risk management exercise. But I want to know that they're compliant, okay? So please give the committee a rundown of each of those 14 companies—the details of those companies and if they are compliant with the essential eight and top four.

Answer:

Defence requires that all companies handling sensitive or classified information be members of the Defence Industry Security Program (DISP) and meet all Defence security requirements. All members of the Industry Vetting Panel (IVP) are members of the DISP. Information provided to the IVP providers is handled in accordance with Defence security requirements, which includes mandatory information, communication and technology controls.

The 14 IVP companies currently assigned to complete positive vetting cases are accredited against the Australian Signals Directorate (ASD) Top Four cyber security requirements. This is a mandatory compliance under the DISP. Compliance with the ASD Essential Eight is not mandatory. Achievement of non-mandatory elements of the ASD Essential Eight is managed through an ongoing process of information, communication and technology review and audit.

Joint Committee of Public Accounts and Audit

Parliamentary inquiry – Auditor-General's reports 38 and 43 (2017-18) –
17 August 2018

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: JCPAA - Auditor-General's reports 38 and 43 (2017-18) - 17 August 2018 - Q4 -
Percentage of clearances denied or downgraded - Senator Smith

Question reference number: Number 4

Senator: Dean Smith

Type of question: Spoken

Date set by the committee for the return of answer: 14 September 2018

Question:

Mr Fortune: Based on reporting either from the agency's security officers or through the individual declaring a change in their circumstances, we triage those cases through a risk based profile and institute a review for cause. We'll deny or downgrade around 50 to 80 clearances annually. A percentage of those are based on self-reporting and/or, more importantly, agency security officers reporting a change of circumstances which causes us to review the suitability of that clearance level, and an outcome may be—and has been—to deny, revoke or downgrade that clearance level.

CHAIR: What proportion? You said 'a percentage'; what percentage?

Mr Fortune: I'll take on notice the specific percentages of our reviews for cause. We do around 50 to 80 denies/revokes a year.

Answer:

AGSVA may deny, revoke or downgrade a security clearance following a security clearance assessment, a revalidation of an existing security clearance, or in response to a "Review for Cause" - a security clearance review generated by an adverse "change of circumstance" report or other security-related referrals to AGSVA. In the period reviewed by the Australian National Audit Office (2015-16 to 2016-17), 18 per cent of security clearances that were denied, revoked or downgraded were the result of a Review for Cause (24 clearances).

Joint Committee of Public Accounts and Audit

Parliamentary inquiry – Auditor-General's reports 38 and 43 (2017-18) –
17 August 2018

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: JCPAA - Auditor-General's reports 38 and 43 (2017-18) - 17 August 2018 - Q5 -
Contractors - Hill

Question reference number: Number 5

Member: Julian Hill

Type of question: Spoken

Date set by the committee for the return of answer: 14 September 2018

Question:

Mr HILL: For, let's say, John Smith, a senior officer with positive vetting, there would be a record that a security clearance was done for a person called John Smith, retained by the contractor forever?

Mr Fortune: Well, I'd have to take on notice exactly

...

Mr HILL: So my question remains: why do you need to have private contractors retain lists of names of people who have been spoken to as part of positive vetting of senior sensitive operators?

Mr Fortune: I'll have to take on notice the detailed information that you're asking about.

Mr HILL: Thank you.

Answer:

Defence requires that all companies handling sensitive or classified information be members of the Defence Industry Security Program (DISP) and meet all Defence security requirements.

All members of the Industry Vetting Panel (IVP) are members of the DISP. Security related information provided to the IVP providers is handled in accordance with Defence Industry security requirements.

IVP companies ensure all documentation relating to a clearance process is attached to the appropriate Personal Security File (PSF) and returned to AGSVA when a case is completed. When the PSF is returned to AGSVA, companies immediately destroy any hard copy duplicates of information that was included in the PSF.

Electronic documentation can be kept on an Information and Communication Technology (ICT) certified system for up to 90 days after the PSF is returned to AGSVA. This allows for AGSVA to obtain further or missing documentation, if required, during the decision making stages.

To ensure adherence to this directive, companies are subject to random checks of ICT storage systems as part of AGSVA audit processes and performance review meetings.

Joint Committee of Public Accounts and Audit

Parliamentary inquiry – Auditor-General's reports 38 and 43 (2017-18) –
17 August 2018

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: JCPAA - Auditor-General's reports 38 and 43 (2017-18) - 17 August 2018 - Q6 -
Entities working for foreign countries - Brodtmann

Question reference number: Number 6

Member: Gai Brodtmann

Type of question: Spoken

Date set by the committee for the return of answer: 14 September 2018

Question:

Ms BRODTMANN: Following on from Mr Hill's comments, you said that none of those 14 entities that are doing positive vetting for government agencies do any work for foreign countries?

Mr Fortune: That's correct.

Ms BRODTMANN: What's the assurance that you have in place for that?

Mr Fortune: Part of the management of the panel is increasing oversight around foreign ownership and control. So that's a Commonwealth procurement requirement.

Ms BRODTMANN: On notice, can you give us the details about that assurance process so that you can put your hand on your heart and say, 100 per cent, none of them do any work for other nations?

Mr Fortune: That's my understanding and I'll take on notice to provide that absolute assurance.

...

Ms BRODTMANN: These are small entities, they're small outfits, they're small businesses—

Mr Fortune: Small to medium enterprises and sole traders.

Ms BRODTMANN: So they're not owned by any parent companies that are international companies? They're not subsidiaries of those?

Mr Fortune: The detail of that—

Ms BRODTMANN: If you can provide that as well, please.

Answer:

All 14 companies that provide AGSVA Positive Vetting services are members of the Defence Industry Security Program (DISP). DISP accreditation requires an assessment of Foreign Ownership, Control and Influence. No current Industry Vetting Panel (IVP) company

has foreign ownership or identified issues with foreign engagement. DISP companies are required to report annually on the terms of their Defence security accreditation.

Further security assurance is provided by AGSVA's contractual arrangements (Deed of Agreement) with vetting companies, which specifies that no classified information or official material furnished or generated under the Deed of Agreement can be disclosed to any third party.

Under the Deed of Agreement, companies must comply with all relevant Defence policy, including Defence security policy and declaring any actual, potential and perceived Conflict of Interest. No company has advised of any Conflict of Interest.

Joint Committee of Public Accounts and Audit

Parliamentary inquiry – Auditor-General's reports 38 and 43 (2017-18) –
17 August 2018

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: JCPAA - Auditor-General's reports 38 and 43 (2017-18) - 17 August 2018 - Q7 -
Outsource and in-house vetting - Brodtmann

Question reference number: 7

Member: Gai Brodtmann

Type of question: Spoken

Date set by the committee for the return of answer: 14 September 2018

Question:

Ms BRODTMANN: On the outsourcing and in-housing of positive vetting, does the department work out who will be outsourced and who will be vetted in-house? I get my colleague's comment on the more senior people in government agencies—whether their personal information is whizzing around on a pushbike courier to an entity or whether that is done in-house. Can you just give us an idea about how you determine who is outsourced and who is in-housed?

Mr Fortune: We allocate a priority against a workflow. There is consideration of the sensitivity of the clearance subject, but I'll take on notice a more informed response about that process.

Answer:

All vetting providers – AGSVA's Australian Public Service staff and Industry Vetting Panel (IVP) company staff – are appropriately trained and qualified. They are authorised to undertake vetting of all clients.

Defence requires that all IVP companies be members of the Defence Industry Security Program (DISP) and meet all Defence security requirements for handling and storing sensitive or classified information.

Positive Vetting (PV) cases are allocated to the next available vetting officer (contractor or in-house) in the regional office or capital city closest to the person requiring the PV clearance.

Allocation of VIP or potentially sensitive cases is determined on a case-by-case basis.

Joint Committee of Public Accounts and Audit

Parliamentary inquiry – Australian Government Security Arrangements: Personnel Security and Domestic Passenger Screening – Inquiry based on Auditor-General's reports 38 and 43 (2017-18)

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: JCPAA – Audit Report 38: Mitigating Insider Threats through Personnel Security – 17 Aug 18 – Q1 – AGSVA Vetting Costs – The Committee

Senator: David Fawcett

Type of question: Written

Date set by the committee for the return of answer: 28 September 2018

Question:

For the financial years 2015-16, 2016-17 and 2017-18, please provide the following:

- 1) What is the average cost of a contractor providing the following vetting checks:
 - a. Baseline vetting.
 - b. Negative vetting 1.
 - c. Negative vetting 2.
 - d. Positive vetting.

- 2) What is the highest and lowest cost for a contractor providing the following vetting checks:
 - a. Baseline vetting.
 - b. Negative vetting 1.
 - c. Negative vetting 2.
 - d. Positive vetting.

- 3) What are the cancellation fees for a contractor providing the following vetting checks:
 - a. Baseline vetting.
 - b. Negative vetting 1.
 - c. Negative vetting 2.
 - d. Positive vetting.

- 4) With regard to Questions 1-3, please also provide additional information, if necessary, for the various stages (Initial/Upgrades, Revalidations).

Answers:

1) The average cost of contractor-provided vetting services for initial/upgrade and revalidation clearances is detailed in Table 1.

| | 2015/16 | 2016/17 | 2017/18 |
|---|------------|------------|------------|
| Average cost (Initials/Upgrades) | | | |
| Baseline | \$307.41 | \$315.05 | \$321.67 |
| Negative Vetting 1 | \$634.87 | \$650.65 | \$664.33 |
| Negative Vetting 2 | \$1,416.42 | \$1,451.62 | \$1,482.13 |
| Positive Vetting | \$4,513.28 | \$4,625.46 | \$4,722.68 |
| Average cost (Revalidations) | | | |
| Baseline | \$295.88 | \$303.24 | \$309.61 |
| Negative Vetting 1 | \$589.65 | \$604.30 | \$617.00 |
| Negative Vetting 2 | \$1,350.50 | \$1,384.07 | \$1,413.16 |
| Positive Vetting | \$4,449.25 | \$4,500.83 | \$4,595.43 |

Table 1. Average cost of contractor services for initials and upgrades by clearance level.

2) The highest and lowest costs for a contractor providing vetting services are commercial-in-confidence and cannot be released publicly.

3) The cancellation fees for a contractor providing vetting checks are calculated on a percentage of work completed basis, as shown in Table 2. This is in accordance with the Deed of Agreement.

| Cancellation stage | % of Total Fee |
|---|----------------|
| Pack received, examine and review case material, identify all gaps, anomalies and discrepancies | 20% |
| Request for information from clearance subject, referee and supervisor interviews | 50% |
| Case Assessment and Clearance Subject Interview (if applicable) | 75% |
| Final Report | 100% |

Table 2. Cancellation fee percentages

4) Nil response.