IGIS
Inspector-General of
Intelligence and Security

Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority and related matters

Dr Vivienne Thom
Inspector-General of Intelligence and Security
under the *Inspector-General of Intelligence and Security Act 1986*

December 2011

Executive summary

On 16 May 2011 three former contractors who had been employed as data-entry operators in Defence Security Authority's (DSA's) Brisbane-based vetting operation made allegations on the ABC *Lateline* program of inappropriate vetting practices. The Prime Minister requested the Inspector-General of Intelligence and Security to inquire into the allegations. The inquiry commenced in June 2011.

The inquiry focussed on the allegations of inappropriate vetting practices rather than the human resource management issues that were also raised. Following the *Lateline* disclosure several former and current staff members came forward with further information. The three complainants were interviewed as well as a number of current and former DSA employees and contractors and the inquiry had regard to a wide range of information including systems audits.

Evidence provided to the inquiry confirmed that the substance of the allegations was true: incorrect data had been inserted in the vetting process. Difficulties in uploading data led to the use by vetting staff of 'workarounds' to address both database incompatibilities and situations where an applicant had not provided all of the data required. This corrupted data had then entered the Australian Security Intelligence Organisation (ASIO) and was used for security assessments. The practice was not confined to the three complainants; most if not all staff used workarounds to some extent. There was a wide variation in the use of incorrect data and little by way of documentation. Further, except in limited circumstances, the use of the modified data had not been agreed by ASIO. There was also no support for the suggestion that this data was used as a place marker to be corrected at a later stage.

In the course of the inquiry other practices and incidents, unrelated to data entry, were also identified which were not consistent with good administrative practice.

While there was no evidence that there had been any attempt to subvert or mislead the security clearance process, the report identifies a number of contributing factors that led to these practices including:

- delayed and inadequate systems upgrades
- inadequate formal documentation and manuals
- inadequate training for contractors and APS staff
- the use of delegates who had not completed formal qualifications
- poor systems and process change management
- inadequate quality assurance
- inadequate management oversight and contractual arrangements
- sustained pressure for output following increases in demand.

The Inspector-General found that the integrity of data in both DSA and ASIO had been undermined if not compromised. Modified data entered the databases and some persists today.

The ASIO security assessment is one part of a broader assessment of a person's suitability to hold a clearance. For high-level clearances the process involves a personal interview, multiple referee checks, intrusive financial checks, police record checks and often a psychological interview. This thorough assessment process is designed to pick up issues of security concern. As the data relating

to an individual primary applicant would usually be accurate and complete and was less likely to have been modified, most of the overall clearance process would not be affected by these changes in data.

It was not possible for the inquiry to determine whether any particular ASIO security assessment had been compromised. The extensive remediation work currently underway in DSA should identify whether any cases exist.

Although lack of management oversight contributed to the problems in DSA, the Inspector-General did not form the opinion that there was sufficient evidence that any person was guilty of a breach of duty or of misconduct to justify referral to the Secretary of the Department of Defence.

The Inspector-General noted that senior executive officers hold leadership positions of special responsibility and accountability. While acknowledging the workload at the time she observed that although it may be appropriate for senior executive officers to rely on the advice of subordinate officers to some extent, this does not diminish the individual personal responsibility or accountability of individual senior executive officers. In particular, senior executive officers cannot rely only on information they receive – they also need to actively assure themselves in whatever way they can that advice is complete and accurate and that they understand its significance.

The Department of Defence has advised that remedial action is underway. The Australian Government Security Vetting Agency (AGVSA) has commenced validation of information required for ASIO security assessments granted since 2009. If validation identifies that information has been changed without justification then the correct information will be obtained from the clearance holder and provided to ASIO under an agreed data remediation strategy. The nature of any data discrepancies may require clearances of concern to be revalidated by AGSVA and ASIO. All vetting documentation is now being reviewed to ensure that it is authorised and fit for purpose, is applied consistently and is readily available to all staff.

On the basis that this remediation work will be conducted expeditiously, the Inspector-General makes no further recommendations relating to remediation of existing security clearances.

Potentially the most significant outstanding issue is that remediation will not resolve all data issues – particularly those relating to the unauthorised and unaudited access to the current electronic vettee pack where it seems likely that it will not be possible to identify the missing or inaccurate information. Defence advises that IT fixes should resolve known problems with transferring data between systems. Defence is also limiting access to a mechanism that potentially allows unaudited changes to vettee information to a very small number of authorised staff.

The Inspector-General also makes no recommendations in relation to a review of management structure noting that this is being considered as part of an internal Defence review.

In the *Lateline* program the complainants alleged that they had raised data integrity issues in previous DSA reviews. Although such issues were raised in reviews focussed on staff management issues, the warning signs were not heeded by senior management.

Defence has accepted all recommendations.

Recommendations

Recommendation 1
The Department of Defence should write to the three *Lateline* complainants and acknowledge that their allegations in respect of data-entry were true.

Recommendation 2
The AGSVA should review the adequacy of its IT systems user controls and audit capability and take appropriate remedial actions where necessary.

Recommendation 3
The Defence Chief Audit Executive should review and report annually on the AGSVA's compliance with all applicable Government security vetting policies, with the first review to be completed by 30 June 2012. The results of the reviews should be reported in Defence's annual report. The need for annual reviews should be reconsidered after three years.

Recommendation 4
All business processes, policies and procedures, including any workarounds, should be appropriately documented and be in accordance with the relevant legislative requirements. Documentation should be formally authorised by DSA management, endorsed by ASIO (where relevant), and subject to version control. Documents should be readily available, and appropriate for their purpose and audience.

Recommendation 5
A comprehensive Training Needs Analysis should be conducted in the AGSVA and a structured training program introduced to cover all aspects of training from induction to ongoing development and education, with a view to professionalising the vetting workforce.

Recommendation 6
All staff involved in vetting in the AGSVA, up to and including EL2 level officers, should be required to hold a recognised qualification in security vetting. Qualifications held by staff should be appropriately confirmed and recorded in the relevant IT systems.

Recommendation 7
The AGSVA should formalise change-management processes for policies, procedures, and systems. Changes should be appropriately communicated, centrally-recorded and adequate resources allocated to training programmes.

Recommendation 8
The AGSVA should implement a Quality Management System to cover the full-range of activities involved in a security clearance process.

Recommendation 9
Defence should review contracting arrangement in the NCC with the aim of ensuring that contract personnel can be subject to appropriate APS management oversight and that all staff can be subject to common policies, procedures, training and performance management including being held to the same standard of conduct.

Recommendation 10
Defence should review whether the staffing numbers for the NCC/AGSVA are adequate given the growth in security clearance requirements within the Australian Government in recent years and the failure of systems to deliver projected productivity improvements.

Recommendation 11
The implementation of PSAMS2 should be given a high priority in Defence's ICT program.

Recommendation 12
The AGSVA should work with ASIO as a matter of urgency to resolve the outstanding data transfer compatibility issues and agree and document any appropriate workarounds.

Recommendation 13
When a clearance is due for re-evaluation, the vettee should be explicitly notified that the data may be corrupt and informed of their obligation to correct it.