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

Contents

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.

Glossary

AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
APS	Australian Public Service
ASIO	Australian Security Intelligence Organisation
ASV	Assistant Secretary Vetting; previously classified as Executive Director Vetting (EDV)
CIOG	Chief Information Officer Group, within Department of Defence
CML	Careers Multi-List
CSO	Chief Security Officer
CVU	Centralised Vetting Unit
DRMS	Defence Records Management System
DSA	Defence Security Authority
DVO	Director Vetting Operations
DVS	Director Vetting Support
EDV	Executive Director Vetting; later reclassified Assistant Secretary Vetting (ASV)
EL	Executive Level (employee)
IGD	Inspector-General Defence
IGIS	Inspector-General of Intelligence and Security
IGIS Act	*Inspector-General of Intelligence and Security Act 1986*
IVP	Industry Vetting Panel
NCC	National Coordination Centre
NV/NV1/NV2	Negative Vet, Negative Vet1, Negative Vet2
PSA	Principle Security Advisor
PSAMS	Personnel Security Assessment Management System
PSF	Personnel Security File
PSM	Protective Security Manual
PSPF	Protective Security Policy Framework
PV	(Top Secret) Positive Vet
PVPI	Positive Vetting Process Improvement
SOP	Standard Operating Procedure
TSPV	Top Secret Positive Vet

Part 1 The basis of the inquiry

THE *LATELINE* DISCLOSURES

On 16 May 2011, three former contractors who had been employed as data-entry operators in the Defence Security Authority's (DSA's) Brisbane-based vetting operations appeared on the ABC television program *Lateline*. The three, Mr Owen Laikum, Ms Monica Bennett-Ryan and Ms Janice Weightman, made a series of allegations about workplace practices, including allegations of the falsification of data, which they said compromised the Department of Defence (Defence) security clearance process, in particular clearances of private security guards responsible for protecting Australian military bases.

Previously, in March 2010, the three complainants had written to their Federal Member of Parliament alleging a culture of bullying at the DSA. In response Defence had initiated an independent investigation into workplace bullying and harassment. Ms Bennett-Ryan told the *Lateline* program that she had informed one of the investigators about the fabrication of information in Top Secret clearances at that time.

DEFENCE'S RESPONSE TO THE ALLEGATIONS

On 17 May 2011 the Secretary of the Department of Defence tasked the head of Defence's internal fraud and ethics branch, the Inspector-General of Defence (IGD), to undertake an initial assessment to determine whether a full investigation was required. On 18 May the IGD visited the DSA's National Coordination Centre (NCC) in Brisbane where the complainants had worked. Staff at the NCC were invited by IGD to provide information about the allegations under the full protection of the Defence Whistleblower Scheme. IGD also commenced an audit of data entered by the three complainants into Defence's Personnel Security Assessment Management System (PSAMS).

The three complainants were contacted by an IGD investigator. All three complainants advised they had retained legal representation and would not cooperate with any inquiry without a guarantee of immunity from prosecution. Although the IGD could conduct an administrative investigation, the position is not an independent office established by legislation and the IGD is not able to offer any immunity for witnesses from criminal or civil prosecution.

THE IGIS INQUIRY

In light of this impasse, the Minister for Defence then sought agreement from the Prime Minister to refer the investigation to me for an inquiry to be conducted under the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act).

On 29 May 2011 the Prime Minister formally requested that I conduct an inquiry into 'allegations of inappropriate vetting practices in the Defence Security Authority and related matters'.

On 1 June 2011, I wrote to the Prime Minister to accept the inquiry. An inquiry of this kind is provided for under s 9(3) of the IGIS Act which requires me, at the request of the Prime Minister, to inquire into an intelligence or security matter relating to a Commonwealth agency.

Without a request of this kind my oversight is limited to the activities of the six agencies of the Australian Intelligence Community.

The IGIS Act provides the Inspector-General with significant powers with which to conduct inquiries. Section 18 provides that the Inspector-General may:

- compel the giving of information or the production of a document that the Inspector-General has reason to believe is relevant to an inquiry
- compel a person to appear and answer questions where the Inspector-General has reason to believe that they are able to give information relevant to the inquiry
- administer an oath or affirmation to a person appearing and examine the person on oath or affirmation.

Section 18 also provides that it is an offence to fail to give information or produce a document or answer a question from the Inspector-General when required to do so. A person is not excused from giving information, producing a document or answering a question from the Inspector-General on the grounds that doing so would contravene the provisions of another Act, be contrary to the public interest or might tend to incriminate the person, make the person liable to a penalty or disclose legal advice given to a Minister or Commonwealth agency.

However, and particularly relevant to this inquiry, s 18 also provides protections for those persons giving information, producing a document to, or answering questions from, the Inspector-General. Any information which is obtained under s 18 is not admissible in any court or proceedings except in a prosecution for a limited number of offences. Further, a person is not liable to any penalty under the provisions of any law of the Commonwealth or of the States or a Territory by reason only of giving information, producing a document to, or answering a question of, the Inspector-General.

To conduct the inquiry, I established a small team from existing staffing within my office comprising Ms Maryanne Gates and Mr Richard Beyer. Additional funding for travel and administration was provided by Defence.

THE INQUIRY PROCESS

On accepting the inquiry, I prepared a public statement that was distributed to all DSA staff and published on my official website. This statement outlined the provisions of the IGIS Act that allowed me to conduct the inquiry, and identified the powers and protections that applied. The statement also invited public comment from anyone with any information relevant to the inquiry. I also issued a notice under s 18(1) of the IGIS Act to the IGD for the production of all the material collected in the course of his initial inquiry.

In response to the announcement and the work done by the IGD, several former and current APS and contract staff from across the DSA came forward to offer written statements or request an opportunity to be interviewed under oath. This work also identified a number of line managers from both the NCC and the DSA Canberra who were either in key positions at the time of the complaints, or were assessed to have information relevant to the inquiry.

Information for the inquiry was obtained mainly by interviewing current and former DSA staff and contractors. In total, 23 notices were issued under s 18(3) of the IGIS Act, directing individuals to attend before me to answer questions relevant to the inquiry, and 13 notices under s 18(1) of the

Act requesting written statements or the production of documents. Included in the 23 interviewees were the three original complainants.

The IGD also provided some supporting data upon request throughout the inquiry, including the results of the audit conducted by his staff on the clearances processed by the three original complainants which was received by my office on 27 September 2011.

I would like to acknowledge the cooperation of current and former Defence staff and contractors, and the efforts of IGD staff in particular, in responding to my requests for information.

Initially, I had hoped to complete the inquiry within three months; however, after interviewing a number of DSA staff it became apparent that allegations of inappropriate practice were far more widespread than initially anticipated.

Where I propose to set out in a report opinions that are, either expressly or impliedly critical of a person, s 17(5) of the IGIS Act requires me to 'give the person a reasonable opportunity to appear before [me] and to make, either orally or in writing, submission in relation to the matters that are the subject of the inquiry'. On 12 September 2011 I informed a number of individuals of my preliminary views and invited them to make submissions. These further submissions were all received by 26 September 2011.

The legislation also requires me to allow the head of an agency a similar opportunity to comment. I informed the Secretary of the Department of Defence of my preliminary views on 28 September 2011 inviting him to comment. I met with the Acting Secretary on 4 October 2011 and received formal comments on 7 October 2011.

On 14 October 2011 I provided the Secretary with a draft report for comment. The legislation also requires me to give the responsible Minister a reasonable opportunity to discuss the proposed report if the report sets out opinions that are, either expressly or impliedly critical. I met with the Minister for Defence on 19 October 2011. Following receipt of agency comments the report was finalised and provided to the Prime Minister, Minister for Defence and the Secretary of the Department of Defence.

EARLIER WARNING SIGNS

Ministerial correspondence

On 22 March 2010 Ms Bennett-Ryan met with her Federal Member of Parliament to discuss her complaints against the DSA. At this meeting she provided her Federal Member with a letter, dated the same day, which included the following:

> There are other staff wanting to come forward but who feel constrained by the Secrecy Act and so, on their behalf, I request legal clarification of the following questions:
>
> - What happens when the Secrecy Act [sic] prevents the exposure of the breaking of security protocols?
> - What happens when the Secrecy Act prevents witnesses from speaking out about breaches that can cause serious harm to National Security?
> - How can a public servant working within a high level of security speak out against practices that are potentially placing Military Bases and Armaments at risk without incurring criminal prosecution?

- Does the Secrecy Act provide an exemption to those who wish to prevent harm to Australia, its government and its Defence Forces?

Ms Bennett-Ryan's letter, covering five separate letters of complaint about bullying and discrimination from ex-contractors including Ms Bennett-Ryan, was forwarded to the Minister for Veterans Affairs and Defence Personnel. The Federal Member's covering letter to the Minister dated 6 May 2010 states:

> Ms Bennett-Ryan has:
>
> - Concerns about bullying and discrimination at this workplace; and
> - Concerns that the Secrecy Act [*sic*] restricts taking action on these concerns.

Correspondence to the Minister for Veterans Affairs and Defence Personnel approved by Defence's Chief Security Officer, Mr Frank Roberts, on 24 May 2010 advises the following actions taken by Defence in response to the letter:

> The complaint has been made against both Recruitment@Top and the Defence Security Authority. I have directed that an independent investigator be appointed to review this matter with a full report to be provided by 15 June 2010.
>
> The Secrecy Act [*sic*] does not prevent anyone employed in the Defence Security Authority from making workplace complaints to their supervisors. I have asked that an email be sent to all National Coordination Centre staff, both Australian Public Service and contracted staff, making this clear and encouraging them to raise any workplace concerns.

While Ms Bennett-Ryan's letter of 22 March 2010 suggests there are concerns about 'breaches that can cause serious harm to National Security', the correspondence to the Minister on 24 May 2010 indicates the Defence response focussed on the concerns as raised in the covering letter dated 6 May 2010, that is the complaints of bullying and discrimination and the concern that secrecy provisions restricted staff from raising workplace issues.

While it is unfortunate that Defence did not pick up on the implied concerns about security issues in Ms Bennett-Ryan's letter, it did refer the matter in its entirety to an independent investigator, and Defence also addressed the immediate concern to ensure that secrecy considerations would not deter staff from raising workplace issues.

The Brennan reports

Ms Bennett-Ryan had told the *Lateline* program that she had informed one of the investigators conducting an investigation into bullying and harassment claims in 2010 about the fabrication of information in Top Secret clearances at that time. In the course of preliminary information gathering, I was provided with two reports as a result of the investigations commissioned by Defence in 2010. At interview in August 2011, Mr Peter Sinfield, Assistant Secretary Vetting (ASV), stated he initiated the investigations following a series of claims of bullying and harassment at the NCC: the first from an APS staff member and then from five ex-contractors (including the three *Lateline* complainants).

A Canberra based firm, Robert Brennan and Associates, was appointed in June 2010 to conduct two investigations; the first by Ms Julie Trent to address complaints of bullying and harassment and the second by Mr Robert Brennan to identify systemic management issues within the DSA.

As alleged by Ms Bennett-Ryan on the *Lateline* report, both she and Ms Weightman had informed Ms Trent of concerns with the security processes at the NCC during the course of that investigation. The report released by Ms Trent in September 2010 states:

> Ms Weightman highlights a number of concerns relating to the security process at NCC, the scope of this project does not allow me to investigate her alleged breaches of process however I would highly recommend that her concerns are taken seriously and that at the very least an internal review is conducted into the particular circumstances that she refers to. This information will be provided separately to DSA for their attention.

It appears Ms Trent did not provide this information, nor did the DSA follow up on this finding in her report.

The second report released by Mr Brennan on 22 October 2010 focuses primarily on management issues and concluded that 'the NCC shows serious, systemic faults which are adversely affecting staff well-being and morale, and which are likely to have significant negative impact on both productivity and quality of output'.

One former APS staff member advised me at interview that she had raised at least one improper work practice with Mr Brennan which could have led to security concerns. Mr Brennan's hand written notes indicates discussion about this issue took place and the comments were provided with the report.

While these earlier investigations and reports were focussed on HR issues, it is unfortunate that DSA management did not heed some of the warning signs and request further information from Ms Trent and Mr Brennan. In particular, an organisation charged with a security role should have found the observations in Ms Trent's report significant enough to follow up.

Defence has agreed that this was a failure on behalf of those involved.

Part 2 **Background**

MANAGEMENT OF THE SECURITY VETTING PROCESS

There had been significant changes in both vetting processes and organisational structure in the lead up to and following the period when the three complainants were employed at the NCC between 16 June 2009 and 15 February 2010.

Prior to 2007, Top Secret Positive Vetting (TSPV) in Defence was conducted by the Directorate of Positive Vetting within the DSA in Canberra. Negative Vetting (NV), which covered Top Secret, Secret, Confidential and Restricted clearances, was conducted by the Directorate of National Operations, which was managed centrally by the DSA in Canberra but also had regional offices.

In 2006 the Positive Vetting Process Improvement (PVPI) review was commissioned by Defence to examine ways to streamline the TSPV process. The delays in receiving a TSPV clearance were causing considerable concern for Defence and in particular the Defence Intelligence Agencies. Additionally, re-evaluations had been largely on hold for several years to concentrate on initial clearances.

The PVPI review was finalised in September 2006 and the recommendations agreed to by Defence. These recommendations primarily involved a move away from an APS6 vetting officer conducting a TSPV security clearance from start to finish, to referee interviews being allocated to APS 4/5 vetting officers in the regions with the results consolidated by an analyst in Canberra.

In 2007 Defence combined TSPV and NV operations in the DSA, under an Executive Director Vetting, to take advantage of economies of scale and to try to reduce the backlogs of NV clearances and TSPV re-evaluations (reported to include about 30 000 NV clearances at the time). This was followed by significant structural changes in 2008 to streamline operations. The new structure included a Director Vetting Operations (DVO) and a Director Vetting Support (DVS) at the EL2 level in Canberra. The NCC in Brisbane had the primary role of data entry for all level of clearances while the National Aftercare Centre, now called the Vetting Support Centre, in Adelaide managed aftercare.

Also in 2007, the Industry Vetting Panel (IVP) contract was established to provide Defence with a panel of private vetting companies to assist with the ever increasing number of security clearances. These vetting companies conducted interviews and prepared recommendations; however, the decision whether or not to grant a security clearance was made by the DSA.

In November 2009 Defence was tasked with establishing a Centralised Vetting Unit (CVU) to provide vetting services to Commonwealth Government agencies, and an SES Band 1 position, Assistant Secretary Vetting (ASV), was subsequently established within the DSA to implement the proposal. This position was filled by Mr Peter Sinfield.

Anticipated productivity enhancements resulting from proposed systems improvements were factored into planning for the CVU. While a fully functioning and robust electronic vetting system has still not been realised, the Australian Government Security Vetting Agency (AGSVA) was established on 1 October 2010.

In June 2010 the Australian Government launched its new Protective Security Policy Framework, to coincide with the formation of AGSVA. The framework replaced the Commonwealth Protective Security Manual (PSM) with a range of core standards, policies and guidelines, including the *Australian Government Personnel Security Core Policy*. The policy also outlined changes to the levels of vetting as follows:

Level of Vetting:	**Access to:**
Baseline Vetting	PROTECTED
Level 1 – Negative Vetting (NV1)	PROTECTED, CONFIDENTIAL & SECRET
Level 2 – Negative Vetting (NV2)	PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET
Positive Vetting	All classification levels including certain types of caveated and codeword information

The *Personnel Security Practitioners Guidelines* and *Australian Government Personnel Security Protocol* were released in September 2010 and January 2011 respectively, and provide more detailed advice on mandatory personnel security requirements. The protocol applies to baseline and NV security clearances, while PV security clearance protocols are managed by the Australian Intelligence Community through the Inter-Agency Security Forum.

In this report I have used the term 'DSA' as it includes both the Vetting Branch (pre-October 2010) and the AGSVA (post-October 2010). I recognise that the DSA also includes branches and functions not connected to vetting but this report does not address those functions.

I recognise that there were a number of other significant activities underway in DSA in 2009/10 that competed with the vetting function for management attention. The Chief Security Officer, Mr Frank Roberts, advised me that the two principal activities at the time were responding to the allegation that Defence was spying on Minister Fitzgibbon and work to improve base security following the arrest of individuals planning an attack on Holsworthy Barracks.

THE NATIONAL COORDINATION CENTRE

The main roles of the NCC are:

- initiating clearance processes on request from sponsors
- receipting and data entry (either manual or electronic) of completed packs
- conducting security clearance processes (for example conducting checks and coordinating the conduct of interviews)
- recommending and granting of NV clearances.

The NCC is managed by the Assistant Director NCC, which is an EL1 position reporting to the DVO (EL2) at the DSA in Canberra.

The DSA was not able to provide me with an NCC organisational chart during the relevant period, however I am advised that in 2009/10 it consisted of three teams, each headed by an APS6, then referred to as Principal Security Advisors (PSAs).

I am advised that during the relevant period there were approximately 45 staff at the NCC, including both APS and contractors. Prior to 2008, lower level tasks such as administration and data entry were conducted by APS3s. However, it was subsequently decided to source contract

staff to carry out this work, in order to free up APS staff to conduct analytical work and on the understanding that these lower level tasks would not be required following planned system upgrades.

Following an initial contract in 2008, the current contract was signed in January 2009 with Adelaide-based recruitment company, CareersMultiList (CML). From 2009 CML subcontracted Recruitment@Top, a Brisbane based firm, to provide contract staff for the NCC. The three *Lateline* complainants were employed by Recruitment@Top through this arrangement.

I am advised that during 2009/2010 there were approximately 20 contractors working at the NCC, primarily in the areas of administrative support and data entry. Contract conditions required that they were only to be employed on low risk, manual tasks and should not be used in decision-making roles. The contractors were paid an hourly rate as casual employees. The labour hire agreements signed by contractors allowed for their 'assignment' to be cancelled at very short notice, for example if they did not meet quotas and guidelines set by CML and Defence. I was advised by contractors that generally, they would be advised at the end of a work day if they were not required the following day.

Accommodation at the NCC was an ongoing issue until their move to new accommodation in July 2011. In 2009, staff were spread across three floors of a building in Victoria Barracks on the outskirts of the Brisbane CBD. The building was old, it had no lifts and steep stairs which resulted in occupational health and safety considerations for the movement of the large number of files that were an everyday part of business at the NCC. As staff numbers increased, not everyone had a desk and there were ongoing problems with air-conditioning.

In 2010 some NCC staff were moved into another building also in Victoria Barracks. Despite being refurbished for the NCC, it had narrow, steep stairs and corridors leading to numerous small office spaces. There were also problems with air-conditioning. Most of the contractors were moved to this building along with two APS staff. There were claims this was a deliberate move to separate APS and contract staff; however, DSA management advised the decision was related to work function, and indeed some contractors remained in the main building.

In July 2011 the NCC moved to leased accommodation in a commercial building in nearby Roma Street, which appears to have resolved the accommodation issue.

DSA SYSTEMS

PSAMS: Defence introduced the PSAMS database in November 1997 to support the vetting process. The database stores clearance holder information such as biographical data and details of relatives, education, employment, overseas travel, finances and associations. It also holds information on the actual clearance, such as the sponsor, justification, results of external checks, recommending and granting officer, date granted and due date for revalidation or re-evaluation.

PSAMS incorporates technologies that are no longer supported by the original vendors. Data validation in the system also reflects the age of the technology and the fact it was originally intended as a data storage system. As a result, there are negligible data quality checks built into the application and the same piece of information can be represented in different ways depending on the preference of the data entry operator.

Defence acknowledges that PSAMS is an out-of-date system. The DSA has been working to have the system upgraded since 2007 but this has not been given a high priority within Defence.

ePack: This web-based interface was first introduced in 2004 and allows applicants to enter their own information into a staging system. Once the applicant had entered all mandatory information they could submit their data. This would subsequently be uploaded into PSAMS. Until September 2010 ePack was only available on an internal Defence network and therefore applicants outside of Defence were still required to submit hard copy paper forms.

THE SECURITY CLEARANCE PROCESS

Prior to June 2010 the security clearance process for the Commonwealth was prescribed in Part D of the PSM. This has now been superseded by the Protective Security Policy Framework, however the process remains largely unchanged. The process varies depending on the level of clearance, primarily in regard to the requisite checking period and the number of checks and interviews required.

The process is generally initiated by a request for a clearance by a sponsor, and a 'pack' is sent to the applicant. Prior to 2004 this was in the form of a paper document, but over time the DSA has transitioned to ePack. Depending on the level of clearance, the pack includes the following forms:

- Request for Clearance
- Personal Particulars
- Financial Declaration
- General Consent
- Official Secrecy
- Consent to Obtain Personal Information – Full Exclusion
- Statutory Declaration
- Referee Contact Details.

The applicant is required to return the completed forms to the DSA, as well as copies of mandatory documentation, including:

- Full birth certificate
- Marriage certificate
- Divorce documents
- Change of name certificate
- Naturalisation/citizenship certificate
- Passports.

The General Consent, Official Secrecy, Personal Particulars and Statutory Declaration forms must be correctly witnessed to be valid and mandatory documentation must be appropriately certified as true copies.

Once a completed pack has been received it is 'co-orded'. This includes checking the pack for completeness and entering the data, primarily from the Personal Particulars form, into PSAMS. In the case of a hard copy pack the data is manually entered and with ePack the data is uploaded.

If the applicant does not provide everything required, the pack is 'rejected' and returned to the person with a request to provide whatever is missing. Often this is due to a missing signature or missing data on the Personal Particulars form (for example a date of birth or address details). In the case of missing data, the applicant might instead be contacted by phone or email to provide the information and the pack annotated to indicate the data was added or modified following advice from the clearance subject.

The co-ord process also includes generating a Personal Security File (PSF) and initiating a series of checks, including an ASIO security assessment, an AFP police records check and financial checks.

Next, interviews may be conducted depending on the level of clearance and whether security concerns are identified. In the case of a TSPV (or if warranted for other clearances) a psychological assessment is also conducted.

Once interviews have been completed and external checks received, an assessing officer reviews the case and makes a recommendation. The criteria by which applicants are assessed as suitable to hold a security clearance are outlined in the *Personnel Security Practitioners Guidelines* and *Australian Government Personnel Security Protocol* as: honesty, trustworthiness, maturity, tolerance and loyalty. Where concerns are identified by an assessing officer, the case is generally deemed 'complex' and referred for further work or to a higher level of approval for decision.

A higher level of approval is also generally required if 'provisional access' is requested, in cases where not all mandatory checks have been returned. This will usually only be approved in high priority cases and where no security concerns have been identified. The final grant is not given until all aspects of the clearance process have been completed.

UPGRADE OF DSA SYSTEMS

During reviews of the both the TSPV and NV security clearance processes in 2006 and 2007, it was identified that both were largely manual, paper based processes and that IT systems and support was lacking. A high level analysis of the existing IT systems was conducted in 2007 which proposed a suggested road map for upgrade to ePack and PSAMS to provide greater automation of vetting processes (both for NV and TSPV).

In November 2007 the 'PSAMS Refresh Project' to upgrade ePack and PSAMS commenced. The upgrade of ePack (ePack2) would make it available to all applicants via the public internet and introduce improved business rules through its user interface to ensure data quality issues were resolved by the applicant before the pack was uploaded to PSAMS. Enhancements to PSAMS (PSAMS2) include electronic records management of PSFs, system facilitated workflow management and improved capabilities for reporting and correspondence.

The anticipated productivity gains from this project were a significant factor in Defence's strategy to manage the AGSVA workload; however, there have been ongoing delays in the project. The ePack upgrade was due to be released in June 2009; however this did not occur until September 2010. Due to pressure to have ePack2 available for the establishment of AGSVA, it was brought into production with a number of unresolved system issues and errors.

I am advised that as at September 2011, the majority of significant problems in ePack2 have been resolved and this phase of the project is soon to be finalised. The PSAMS upgrade was due to be released in March 2010, but is now not forecast to be released until March 2012.

THE DSA-ASIO LINK

An ASIO security assessment is a mandatory check for NV1 or Confidential and above clearances. On request, ASIO provides an assessment of an applicant in relation to national security matters. ASIO assessments are considered by AGSVA when determining the suitability of the clearance subject to access security classified information. The assessment is not the same as a decision to grant a clearance – that remains the responsibility of the AGSVA delegate – but is a recommendation to assist the decision maker.

As well as the upgrade to ePack and PSAMS, there was also a project to develop an electronic link from the DSA to ASIO to facilitate the transfer of data for the purpose of the ASIO security assessment.

Until 2008, the DSA provided ASIO with a hard copy of an applicant's Personal Particulars form to enable them to commence a security assessment. Planning commenced in around 2005 on a DSA/ASIO link to transfer the data required electronically from PSAMS to ASIO. In April 2008, the DSA and ASIO began trialling a semi-automated process, with the data exported from PSAMS and transferred to ASIO via a compact disc. As of 8 May 2009 all data was transferred electronically from the DSA to ASIO in this way. In July 2009, the process was switched to a networked connection between the DSA and ASIO.

For staff at the NCC this meant that once the data from a pack had been entered into PSAMS, they were able to submit the request to ASIO for a security assessment electronically via PSAMS. ASIO would subsequently advise the DSA when the assessment was complete and the details would be populated in PSAMS.

PROJECT GOVERNANCE

The PSAMS Refresh Project is managed by the Chief Information Officer Group (CIOG) under the PRINCE2 methodology with project board oversight. Mr Sinfield represents the DSA as the key client.

Within the DSA, the responsibility for IT systems rests with the Business Technology Manager, an EL1 who, until September 2010, reported to the ASV. The role of the Business Technology Manager included representing the DSA's business requirements to the project team and managing the implementation of the different phases of the project at the DSA, as well as conducting any training required in the new systems and resolving implementation issues. The implementation of the DSA-ASIO link did not appear to have been subject to any formal change-management process within the NCC. There was no discernable process for formally recording errors, nor was there adequate documentation or training provided to users. This is covered in more detail in Part 4 of this report.

DATA INTEGRITY ISSUES AND THE DSA-ASIO LINK

Prior to the introduction of the electronic transfer of data from DSA to ASIO, where there was missing, ambiguous or indecipherable information, ASIO staff would either refer it back to the DSA to resolve with the applicant or resolve it themselves. For example, they might be able to

find the missing street number of a relative's address through the electoral roll. In essence, this process placed the burden of ensuring data quality for the security assessment with ASIO.

The introduction of the electronic transfer of data between the DSA and ASIO resulted in a number of data integrity issues. Business rules designed to ensure mandatory data was provided to ASIO meant that when the data did not meet the required standard, it would be automatically blocked either at the Defence gateway or the ASIO gateway and an error report was generated at the DSA. These were referred to within DSA as *ASIO errors* but will be referred to in this report as *data transfer errors*. I was advised by the DSA that many of these issues had not been identified during the testing phase as ASIO made changes to previously agreed business rules for the network link without notifying the DSA. No evidence was provided to support this.

I was also advised that in the early days of data transfer these error reports were hundreds of pages long, with multiple errors per page. The DSA staff member responsible for resolving data transfer errors for the majority of 2010 told the inquiry 'I basically started with a report that was 145 pages [of data transfer errors], and I brought that report down to 8 pages'.

During 2008/2009 there were regular meetings between the DSA and ASIO at both the business requirements level and the implementation level. The meeting minutes, prepared by ASIO and accepted by the DSA, reflect the ongoing negotiations about data quality. At the crux of the issue was the fact that the data required by the DSA for their vetting purposes was not as comprehensive as the data required by ASIO for the security assessment process. This discrepancy gave rise to some tension between the two agencies and there was a widely held view by some at the DSA, and certainly within the NCC, that not all the data required by ASIO was necessary for the security assessment process. This perception was based largely on the fact that much of the missing mandatory data had not been followed up by ASIO during the era of paper transfer.

ASIO was aware of the issue, but continued to insist on accurate data. An internal ASIO email dated March 2008 from the Assistant Director in ASIO's Security Assessments area explains:

> The reason they have been rarely asked for additional data in the past is not because we don't need it, but because my team has been going above and beyond in finding these details out themselves … and only passing the query to DSA when we couldn't get the details we needed any other way.

The Defence Chief Security Officer, Mr Frank Roberts, has advised the inquiry that he was not aware of ASIO concerns about data and that this had not been raised with him either internally or through his liaison with ASIO in the period 2007-2010.

In September 2008 ASIO attempted to reinforce their message about data quality by sending the Director and responsible Assistant Director of the Security Assessments area to the NCC to explain their requirements. Feedback from senior managers, both at ASIO and at the DSA, was that the visit went well and had been worthwhile. However it appears to have left little subsequent impression on staff at the NCC. The Assistant Director NCC at the time told the inquiry he could not recall the visit and others had only a vague recollection of it.

From April 2008, ASIO did consent to temporarily relax the mandatory data requirements for security assessments. This was formally documented in a letter from the Manager Security

Assessments at ASIO to the Executive Director Vetting (now ASV) at the DSA dated 22 April 2008. It stated:

> … where the Personal Particulars Form is missing information, DSA will undertake all reasonable measures to obtain it from the applicant. However, if DSA is satisfied that the information is not available for a reason that does not affect the applicant's security status, DSA will accept it as unknown and will manage that risk.
>
> In accordance with this proposal, ASIO will accept that the missing information will not affect ASIO's assessment of the subject's suitability to hold a security clearance. ASIO will therefore, as an interim measure, accept and process applications where previously identified mandatory fields are tagged as having unknown data.

Four months later, on 12 August 2008, the Manager Security Assessments at ASIO sent a further letter to the Executive Director Vetting (ASV) at the DSA to formalise the reintroduction of the previously agreed mandatory fields, thereby ending the temporarily relaxed requirement.

Both Mr Roberts (CSO) and Mr Sinfield (ASV) informed me that there is no record of this correspondence ever being received by the DSA. However, the formal minutes of a meeting between ASIO and DSA on 8 August 2008, at which Mr Sinfield was present, states the following:

> AGD therefore requested that mandatory fields be reintroduced as soon as possible, and before electronic referrals were expanded to TSNV and Secret assessments … DSA agreed with this and stated that it will also be working with its Brisbane office to ensure data quality continues to improve.
>
> **Action:** Mandatory fields for electronic referrals to be reintroduced as soon as possible.

Also, a letter from ASIO's First Assistant Director-General, Security Division to Mr Roberts, then Head Defence Security Authority, dated 28 August 2008 regarding the DSA – ASIO External Connectivity Security Project, includes the statement:

> The adjusted timeframe will coincide with the re-introduction of mandatory fields from September …

The 'Head Defence Security Authority' coversheet attached to this letter confirms that both Mr Roberts and Mr Sinfield read the letter and indeed drafted a response and took action based on the content.

Part 3 Alleged inappropriate vetting practices

INITIAL ALLEGATIONS

The allegations about inappropriate vetting practices made in the *Lateline* program included:

- 'falsifying' information
- disregarding missing information and documentation
- adding 'fabricated' information addressing gaps in addresses and employment
- 'rubber stamping' security clearances to 'get the numbers up'.

The complainants alleged that these practices were supported by senior management.

The allegations raised by the original complainants shaped the initial stages of my inquiry. I found that the data-entry practices alleged by the *Lateline* complainants did occur although there was no evidence of any attempt to subvert or mislead the vetting process.

Given this finding, and the fact the Defence had failed to heed earlier warning signs, I think that it is important that Defence should now acknowledge to the *Lateline* complainants that there was substance to the allegations relating to data-entry.

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.

In the course of gathering documents and statements, the range of allegations broadened into a wider range of inappropriate practices and incidents involving the majority of staff at the NCC, both contractors and APS. Some of these practices were generalised throughout the NCC and others were used by specific staff in a specific manner.

It is convenient to categorise the practices broadly as either relating to modifying data or as more generally inappropriate business practices.

Modifying data: Includes practices used to ensure the data entered in PSAMS could proceed through the gateways at Defence and ASIO to allow the request for an ASIO security assessment to get through. The security assessment is a mandatory check for Confidential or NV1 clearances and above. It was also the check that usually took the longest to be completed, therefore was most likely to delay the clearance process. Such practices were subsequently described by DSA staff as 'falsifying data', 'fabricating data', 'workarounds', 'stretching dates' or 'filling gaps'.

Other alleged practices and incidents: Includes alleged practices and individual occurrences of behaviour inconsistent with good administration, but were used generally to prevent delays in the vetting process.

Some of the practices described could be characterised in both groups, but will be dealt with according to the context in which they were disclosed.

MODIFYING DATA

Different levels of clearance have different mandatory information requirements. For example, a Secret or NV1 clearance requires a 10-year chronology of employment, education, travel and residential addresses whereas a TSPV requires 'whole of life' data.

At all levels of clearance, there are standards of data quality imposed by business rules in the various systems used throughout the vetting process. For example, any addresses, whether that of an applicant, family member, employer or educational facility, had to include a street, suburb, city and postcode. Also, any dates, whether it be a date of birth, death, citizenship, arrival in Australia, or travel to a foreign county, for the applicant or otherwise, generally had to include a day, month and year.

It was not uncommon for an applicant's information, whether provided electronically via ePack or otherwise, to have gaps in some of this mandatory information. In some cases the missing information could be attributed to oversight, while in other cases the data might not be available to the applicant. For example an applicant may not know the address of an estranged parent or the date of birth of a relative with whom they have no contact. In other common examples, an applicant may not recall the date of overseas travel or past employment (particularly for whole of life coverage).

Frequently there were gaps in address, education and employment histories, which also caused errors as the DSA-ASIO data link did not accept gaps in some fields. Sometimes there were legitimate reasons for gaps but on other occasions a gap would have no obvious explanation and would need to be explored further during the process.

In cases of missing data, the documented DSA policy required staff to refer back to the applicant to resolve omissions. Either the whole pack was sent back to the applicant or they were contacted to provide the missing information and this was documented on their file.

However, with the significant numbers of data transfer errors generated following the switch to electronic transfer of data and with staff under pressure to clear backlogs, it has become apparent that a number of 'workarounds' eventuated. In some cases staff would legitimately fill in missing data, such as searching for a postcode for a suburb or changing the state from the full name (New South Wales) to the three letter acronym (NSW). While this was acceptable, many of the other practices that developed were not as was later confirmed by managers at the NCC and both previous DVOs in the course of the inquiry.

The Business Technology Manager told the inquiry it was initially his responsibility to resolve the errors resulting from the DSA-ASIO link and he did this through liaison with Team Leaders at the NCC. He stated that it was his understanding that the NCC would develop Standard Operating Procedures. It appears this never happened and no-one checked to ensure it had.

In early 2009 the responsibility to resolve data transfer errors was transferred to an APS3 Team Leader. The information on how to resolve particular errors was then passed to other Team Leaders who would pass it on to their small teams. Often data transfer errors were discussed at regular monthly team meetings and some attendees would take notes. At some point in time formal minutes from these meetings were produced, however these have been largely unable to be recovered and those that were had little detail other than headings, for example 'ASIO Update'.

An email dated 17 March 2010, from the then DVO, advised staff that the Business Technology Manager's role in resolving data transfer errors had ceased and the responsibility now lay with the NCC. A subsequent email from the then Assistant Director NCC to the then DVO notes the data transfer error reports were being resolved by the Recruitment@Top contract Team Leader. The email continues to remark that the Assistant Director NCC did not believe the work was being done at the appropriate level and sought approval to have an APS2 position established within the NCC to do this work. The DVO subsequently forwarded this email to Mr Sinfield, with a request to be allocated time in his diary to discuss. It is not clear whether the meeting took place or if there was any real assessment of the level of judgement required to fulfil this role. However, the work was subsequently assigned to an APS2 officer.

It has been suggested by some staff and senior management that 'dummy data' was put into PSAMS as a place holder, to get the ASIO request to proceed, and staff would correct the data once they had obtained the missing information from the applicant if possible and, if warranted, pass the revised information to ASIO. The small sample of files we reviewed, including a sample of those files that were processed by staff who said they always corrected the data, demonstrated that generally the data was not actually corrected at a later stage. Discussions with ASIO also suggest that, except in limited circumstances, this data was not recognised as a place holder.

The workarounds for missing data are described in detail at Appendix A. As there were so many variations described by NCC staff and we did not interview every current and former NCC staff member since 2008, the list at Appendix A is likely to be incomplete but practices included:

- filling gaps in dates
- resolving overlaps in dates
- using 1/1/1900 (or similar) for missing dates
- creating other dates
- adding street names
- creating addresses and employers
- picking a country.

It was apparent from interviews conducted with NCC staff, both contractors and APS, that they believed they were following instructions from their supervisors rather than 'falsifying' data. I found no evidence that staff had improper motives when modifying data.

OTHER ALLEGED PRACTICES AND INCIDENTS

When I interviewed APS staff and contractors, allegations were made of a number of other practices and incidents that could affect the integrity of the vetting process. These practices are largely unrelated to the ASIO data issues and most seem to have arisen as a result of a pressure for throughput. These alleged practices and incidents are set out in more detail in Appendix B.

Although I have not established the actual extent to which these practices and incidents actually occurred, the fact that so many were readily identified does demonstrate that many staff had serious concerns about the integrity of the vetting process.

Of particular concern is the unaudited use of the ePack password reset function to modify data without reference to the applicant when it did not upload. (This is explained in greater detail in Appendix B). It was estimated that about half of the ePack2 submissions prior to 23 May 2011

may have been affected in this way. Defence queried this high occurrence noting that this could reflect, in part, Customer Service staff using this feature to login with the applicant on the phone prior to pack submission and, with the applicant's consent, look at a specific issue affecting pack completion. While I accept that the figure could include these other instances, it is still a concern that Defence could not provide any audit log.

The practice continued until August 2011. Defence advised in October 2011 that the IT fixes due to be completed by mid-October 2011 should resolve known problems with uploading data from ePack2 to PSAMS. I am advised that until then upload problems would be fixed by requesting the applicant to correct the problem identified by AGSVA staff using a read-only tool to view the ePack. This does not authorise the staff to enter the applicant's pack to change the data.

While the read-only limitation on the administration utility tool prevents staff from entering and changing ePack data, some staff are able to do so using a separate password reset function hosted on the Defence Online Services Domain and administered by the CIOG. The AGSVA is in the process of cancelling access to this tool for all but authorised staff. The number authorised should be very small.

It is apparent that a number of these practices have been able to arise because of inadequate systems controls and audits including lack of user controls such as user access for delegates.

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

In light of these findings it is appropriate that there should be an annual review of the compliance of DSA's practices – particularly as it adopts the necessary changes resulting from this inquiry over the next few years. In my view Defence's Chief Audit Executive would be the appropriate body to conduct the review. Publication of the outcomes of these reviews in Defence's annual report would provide assurance to the Parliament, the general public and other government agencies about the integrity of AGSVA's vetting practices.

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.

Part 4 Contributing factors

In light of the vetting practices found to be occurring at the NCC, the inquiry examined how these inappropriate practices were able to develop and why they were not identified earlier by DSA management.

DOCUMENTATION

One of the most critical failures at the NCC was the lack of appropriate documentation on policy and procedures. When we asked APS staff why the processes were not written down, most stated they were too busy, that things were changing too quickly and the errors would be resolved once the system was fixed. Several staff, both APS and contractors, told us they had requested documentation and this is reflected in some of the evidence provided to the inquiry.

Standard Operating Procedures

Standard Operating Procedures (SOPs) are a fundamental requirement for a process driven organisation, such as the NCC. At the start of the inquiry I was informed that there were SOPs in place at the NCC, including for the workarounds. As the inquiry progressed it became apparent that while some documentation existed, it was not comprehensive, there was no quality control or senior management approval, no version control and no formal process for updating. Furthermore, it was not centrally stored or accessible and it did not cover the workarounds.

The following documentation was provided to me during the course of the inquiry, including any references to the workarounds which were being used:

1. ***DPV Instruction – ADMIN001 Sending and Managing ASIO Checks*** (undated*)* The purpose of this document is described as 'to detail how to send and manage ASIO checks from within PSAMS'. While the document outlines which data fields are mandatory, it does not identify what to do about missing data.

2. ***The Information Book*** (undated). This was developed by a former NCC Team Leader in 2009 in an attempt to compile all relevant information into one manual. It was stored on the 'G: drive' where it was accessible by other staff members. It was amended by the original author 'as changes occurred' until he retired in July 2010.

   I was provided with more than one version of the *Information Book*, as it varied depending on what date it was printed. One of the copies I was provided, which would seem to have been printed in late 2009, had a section titled 'Electronic ASIO assessments'. This outlined some of the accepted business rules, for example the requirement to use agreed acronyms for States and Territories, but did not have any information about workarounds except:

   > For deceased people, date and place of death is required … If they do not know the year, put in 1900.

3. ***Co-ording Reference Guide*** (undated, but advised by NCC as 'pre-August 2009'). This document describes how to co-ord a case, including 'guidelines for PSAMing a case'. There is no mention of workarounds.

4. ***'Top Secrets', 'Secrets', 'Confidentials', 'Restricteds'*** (undated, but advised by NCC as 'post August 2009'). This is a series of instructions for each level of clearance. There is a short section on 'Co-ording' in each, but it does not include any mention of workarounds. There is also a section titled 'ASIO non uploads', which advises that 'Packs held by analysts in the NCC or DSA Regions will receive an email outlining the specific fields to be updated' but does not provide information about *how* to update the fields.

5. ***Meeting minutes and handwritten notes.*** I was provided with various copies of meeting minutes and individual handwritten notes that were put forward as documentary evidence of workarounds. I have reviewed these documents and do not consider they constitute adequate guidance for staff. The meeting minutes were incomplete and generally only included headings of subjects discussed, such as 'ASIO Update'. The handwritten notes were in most cases incomplete, imprecise and barely legible.

6. ***Anecdotal Evidence*** (undated)**.** This document was provided to me in the early days of the inquiry. It did not include an author or the date and the title itself cast doubt about its authority. The document was drafted following the *Lateline* disclosures in the period 22 to 23 May 2011 by five APS Team Leaders at the NCC. I was advised it was drafted at the request of the then acting Assistant Director NCC to be subsequently provided to the Chief Security Officer of the Department of Defence, Mr Frank Roberts. Many of the workarounds described previously in this report are outlined in the document. For example:

   > When the electronic ASIO was introduced different "generic identifiers" were used until DSA/NCC/Analysts/Co-orders were authorised to use NOT SPECIFIED or UNKNOWN and 1/1/1900 by [the Business Technology Manager]/ASIO. These different "generic identifiers" were advised by [the Business Technology Manager]/ASIO and were disseminated to the Analysts and Co-ord from the Team Leaders through discussions either one on one, within the pods and at Team Meetings.

   In the case of many of the workarounds described, the document states that 'the analyst would then follow up with the vettee to obtain this missing information and update PSAMS and forward via email to ASIO'. However, in another example, when a country had been randomly selected because a vettee could not remember what countries they had visited during a Navy deployment, the document states the information 'would be left in PSAMS as is' because it was 'not considered a Security Risk'.

7. ***OPS 16 Entering data into PSAMS for Electronic ASIO Check Requests*** and ***OPS 17 E-Pack Data Collection – Data Entry Protocols*** (June 2011). These documents were drafted in May/June 2011 and sent to NCC staff under cover of an email from Mr Sinfield on 14 June 2011. They were subsequently revoked in late August 2011 by Mr Roberts after he determined that the workarounds contained in these instructions had not been agreed by ASIO. The workarounds described in OPS 16 and OPS 17 are specific to errors in ePack2 and are not related to those described earlier in this report and at Appendix A.

During the course of the interviews I conducted I was unfailingly advised by staff at the NCC, both contractors and APS, that the workarounds they had been using (apart from those in OPS 16 and OPS 17) were not formally documented anywhere and that this had been an issue of ongoing concern for many of them.

Directives

The Assistant Secretary Vetting is authorised by the Chief Security Officer to make determinations on all levels of security clearances. The ASV also issues directives from time to time to facilitate the process. During the course of the inquiry a number of APS staff indicated concern about the implementation of two particular directives:

1. ***Directive 01/10: Granting of Provisional Clearances in Response to Delays in ASIO Security Assessment Returns***. Signed by Mr Sinfield, 28 May 2010. Staff were not generally aware of this directive and its instructions were not reflected in checklists. This is discussed further in Appendix B.

2. ***Directive 01/11: Granting of Provisional Baseline Clearances in Response to Delays in the Return of External Checks.*** Signed by Mr Sinfield, 9 March 2011

   This directive, dated 9 March 2011, instructs staff to:

   > … grant provisional Baseline access to subjects where the clearance subject is a **permanent Australian Government employee** and is awaiting an Australian Federal Police check or referee report [bold added].

   There was confusion following this directive as an email from the Manager Vetting Operations on 11 March instructed staff to 'please ensure any Baselines you are holding are provisionally granted by COB Monday 14 Mar 10'. Clarification was sought whether they were required to 'grant **all** existing baselines' or only 'permanent Australian Government employees.' There was also the question of what constituted an 'Australian Government permanent employee', and how to establish that someone was one. The subsequent advice from the then acting DVO was to:

   > … assume that anything from the Agencies, unless noted otherwise is a permanent Aust Govt employee… Bottom line is the risk at this level is pretty small. [ASV] has assessed the risk and is willing to assume responsibility.

In following up staff concerns about these directives, it became apparent that these were the only two formal directives issued by ASV during the whole of 2010 and to date in 2011, a period of considerable change. The directives were not able to be easily located by DSA staff when copies were requested.

During the course of the inquiry I was advised that ASV 'directives' were more often in the form of an email, usually sent to managers for distribution to their staff. In the course of the inquiry Mr Sinfield stated that he relied on his managers to implement his directives and to raise any concerns surrounding their implementation with him.

Once again, these 'directives' were not able to be easily located because they were not stored in a central location, nor was there a register of policy changes or management directives. It also became apparent that, during recent years at least, the directives were not subsequently incorporated into formal SOPs, making it difficult for staff to keep pace with changes in process and procedures. For example, one such directive released by email by Mr Sinfield on 22 July 2009 to Vetting Branch Managers stated:

> There is a new policy directive coming out shortly which will cover the types of financial checks required for security clearances in line with PSM and [Defence Security Manual] requirements. Until the policy is released, which will hopefully be next week or so, the following directive is to be followed by vetting staff:
>
> - Bankruptcy checks are to be conducted for **Top Secret NV and PV** clearances only. Bankruptcy checks for SECRET clearances are no longer required.

When we requested a copy of the 'new policy directive' we were advised by a senior manager in Canberra that: 'to the best of my knowledge and after consultation with the then Director and Assistant Director Governance it appears that a new policy directive was never actually released'.

Records management

Until the mandatory introduction of the Defence Records Management System (DRMS) at the NCC in September 2009, staff used a shared electronic folder for storing corporate documents. The shared electronic folder, commonly referred to as the 'G Drive' did not include any version or access control or index of records and as such was inadequate as a records-management system. During this time, the DSA's formal records were hard-copy files.

With the introduction of DRMS, NCC staff were encouraged to 'clean up' their electronic holdings. This process resulted in many electronic files, notes, emails and documents being deleted and therefore lost.

During the course of my inquiry it has become apparent that there were few hard copy corporate files or documents produced at the NCC (or the DSA) over recent years. Along with the permanent destruction of electronic records following the move to DRMS it has been difficult to find documentary evidence to piece together events over recent years or to support statements provided during the course of the inquiry. As such, I am compelled to note that corporate record keeping at the DSA is inadequate and represents a serious deficiency in their processes.

Consequences of poor documentation

At the start of the inquiry senior DSA management in Canberra seemed surprised that the SOPs at the NCC were inadequate, particularly in relation to the workarounds. When formally interviewed in July 2011, Mr Sinfield stated:

> We had ops instructions in Canberra. *We* had ops instructions, I believed *they* had SOPs. I had been told we had SOPs up there [in the NCC].

Until August 2011, the advice I received from NCC staff (that workarounds were not documented) contrasted significantly with the advice I was given by senior DSA management in Canberra, that the workarounds *were* documented.

A statement by Mr Roberts dated 9 August 2011, which included some documents not previously provided as well as many of the documents outlined above, includes the comment:

> In practice, as the SOPs could not specify every aspect of an analyst's job, analysts used their training and experience to deal with vetting process matters (such as gaps in information) as they arose.

In this statement, Mr Roberts makes reference to several of the documents outlined above, as 'a factual representation' that documentation of the workarounds existed, including the 'Anecdotal Evidence' document and the hand-written notes following the hand-over from the contractor responsible for resolving data transfer errors in August 2010 to an APS2 officer. The quality and usefulness of these documents has already been discussed in this report and Mr Roberts has subsequently agreed that the documentation was not adequate.

Then, as stated in a Ministerial Submission provided to my office dated 26 August 2011, Defence concluded:

> … the documentation that supported the use of the workarounds was inadequate. Documentation was fragmentary and not comprehensive, and contrary to my initial understanding, there was no single document or instruction that recorded the workarounds.

It is possible to see how an instruction that is not documented can change to become something very different and how over time the methods for 'fixing' data transfer errors became so varied. One staff member noted at interview that it was a bit like 'Chinese whispers'. What may have been a legitimate fix, for example 'use Google to find what state a suburb is in if state is not provided' then seemed to become a case of fabricating data when the instruction was understood to be 'use Google to pick a suburb if only the state is provided'.

I have come to the conclusion that the main reason why the workarounds were not documented was due to the rapid changes that were occurring at the NCC and the lack of importance placed on record keeping, both within the NCC and the DSA in general. This can be summed up by a statement by one of the authors of the 'Anecdotal Evidence' document, when asked why these workarounds were never formally documented:

> Because things were changing so rapidly there was no time to write things down … we never really thought about putting it in an SOP – it became so routine, it was just what we did.

In July 2011, Mr Sinfield advised to the inquiry that the DSA 'had been working on a vetting practitioner's manual ad infinitum'.

Another more concerning reason offered by some current and former staff members at the NCC for why nothing was ever put in writing, was that managers knew the practices were not acceptable. In a written statement, one of the original complainants claimed:

> The very fact that none of this instruction was put into print, the fact that no training information was ever put into print, is a strong example in itself that the practices staff were being told to perform were highly questionable and management didn't want this as an example of their corrupt orders and actions.

The evidence I have obtained does not support this view but, again, the lack of proper documentation and communication has allowed impressions like this to be developed and shared by staff.

The proper documentation of business processes, policies and procedures will be essential for effective and compliant administration in DSA.

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.

TRAINING

Training for contractors

A Brisbane based firm, Recruitment@Top, was sub-contracted by CML to provide the NCC with contractor personnel to undertake basic level administrative tasks, such as filing and data entry.

On commencement at the NCC, contractors received one day of induction training, covering basic administration issues, as well as briefings on security and the role of the NCC. This was followed by role specific, on-job-training provided by an APS staff member. Up until April 2010, there was no dedicated training position in the NCC. The then DVO stated:

> The staff at that stage were taking turns on a voluntary basis, and based on skill as determined by the then acting EL1 … on sitting down and training that person in how you do this particular thing.

Contractors had access to what Standard Operating Procedures existed at the time; however they were not provided with any training manuals and were expected to take their own notes. I am advised that contract staff were closely supervised until it was deemed they were competent.

A number of contractors, including two of the original complainants, advised they had repeatedly requested formal training notes, particularly in relation to dealing with data transfer errors, however they were not forthcoming. Ms Weightman's request for training notes was documented in an exchange between the Recruitment@Top head office and the then contract Team Leader at the NCC:

> If she has her own notes why is she asking to be spoon fed? It appears that you are going down the right track – training the staff to refer to the resources available to them – especially their own training notes which is how they will develop the resources for further information or checking.

Training for APS staff

The senior manager in Canberra who was responsible for training in 2009, and subsequently became DVO in 2010, admitted at interview that the training at the NCC had been inadequate:

> I knew there was a hole there because I hadn't been providing any [training] in my previous role [of Director Vetting Support].

The manager indicated to me that the lack of training was due to the fact that the NCC 'did not welcome advice' from Canberra, and that 'ongoing training and quality circles were already in place'. More specifically:

> As Director Vetting Support, as I said, I am struggling to think where we were invited in to the NCC other than on one occasion, and I think that was around grant delegate training …You weren't allowed to talk directly to staff. You needed to go through [AD NCC] in particular, and when I, the one time I did send training people in, they were escorted.

I do not accept that the relevant manager had to wait to be 'invited' to provide training to the NCC. This statement also indicates an uneasy relationship between managers at the NCC and in Canberra. I also note the same manager advised that the NCC at that time were too busy to allow training:

> ... if training was suggested to [the operations manager], it would come back in terms of - well I would lose 6 years in vetting time if I put everybody out to do that, to do that training.

It was also apparent during the course of the inquiry that training and development was lacking across the board. This appears to include the knowledge and skills required to perform their various roles in vetting, such as mitigating security concerns as assessing officers, as well as more general skills and knowledge such as management and conflict resolution.

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.

Qualifications

A number of APS staff at the NCC indicated concern that assessing officers, both analysts and delegates, were not appropriately trained.

As outlined in the PSM (Section D8, paragraph 3.29):

> Agencies must provide assessing officers with appropriate training recognised by the [Protective Security Policy Committee]. The [Protective Security Policy Committee] and external providers provide such training. Assessing officers, who have not undertaken this training, must not undertake security clearance assessments in Australia.

According to the *Australian Government Personnel Security Practitioners Guidelines:*

> Assessing officers undertaking Negative Vetting Level 2 or complex vetting assessments at lower levels should hold a Certificate IV in Government (Personnel Security) or equivalent. It is also recommended that assessing officers undertaking less complex Negative Vetting Level 1 and Baseline Vetting assessments hold a Certificate III in Government (Security) – *Personnel Security Stream* or equivalent.

AGSVA delegations for managing security clearances are authorised by the CSO and are consistent with these guidelines. A minute dated 2008 relating to Defence's Vetting Branch remains extant. Delegations are assigned by positions or qualification. For staff below the APS6 level a delegate for NV clearances must be 'Certificate IV (Vetting) security trained' whereas to approve all clearances the delegate must be 'Diploma (Vetting) security trained'.

Upon investigation, it became apparent that the policy regarding delegation was not well understood in the DSA, at least at the NV level. There was also some confusion whether the delegation authority related to qualifications, training or APS level. The officer who was responsible for training in their role as DVS and then responsible for operations in their subsequent role as DVO from early 2010, commented at interview:

> …when I took over, there wasn't any clear, I guess, guidelines or rules behind how say, who would grant clearances … In the NCC there was a pod of people who were grant delegates.
>
> Within my regions around the country, the rules on who would grant clearances and who was responsible for things was different in each region. So, I guess I put a standard across that. I imposed, and it is me imposed, I guess, that you need to be Cert III or Cert IV trained depending on the level of clearance.

At interview, Mr Sinfield stated that 'delegates should be Cert IV trained, and analysts should be Cert IV trained'. When asked if an APS3 can be a delegate, he added: 'if they're trained, experienced, yes… It's not a rank base, it's a training and experience and ability to do the job'.

On requesting a list of the DSA staff holding these qualifications, I was initially advised that it did not exist. (Later I was advised that a version dated October 2010 did exist but had not been updated). The DSA generated a current list by requesting that managers in each region fill in a spreadsheet. I subsequently received the list; however it concerns me that the information appears to have come from self-reporting by staff.

The list of staff at the DSA who hold a relevant Certificate III or IV, as provided to my office on 8 August 2011, indicated that the qualification was 'pending' for a significant number of APS staff. Updated figures provided in October 2011 indicated that eight out of twenty delegates had completed some, but not all, components of the Certificate IV qualification. I question whether it is appropriate for staff to be granting clearances without the formal qualification or equivalent, especially over an extended period of time.

In comments provided to the inquiry in September 2011 Mr Roberts asserted that this use of unqualified staff did not amount to non-compliance. The Vetting Branch interpreted the PSM (and presumably their own instrument of delegation) to require vetting staff to undergo 'appropriate training' (as opposed to gaining a full certificate qualification). They seemed to distinguish between the 'formal' training component of the Certificate IV course and the workbook and other modules. I do not agree with DSA's interpretation. In my view, 'Certificate IV training' refers to satisfactory completion of all components including assessment tasks.

Training at the senior management levels was also sporadic. Of the senior staff in the DSA in August 2011, the following were identified as having either a relevant Certificate III or Certificate IV.

	Number with Cert III or Cert IV	Total number of staff at level
SES	0	1
EL2	0	3
EL1	9	24

A significant number of DSA managers advocated, in various forms, the use of workarounds to resolve the error reports arising from the establishment of the DSA-ASIO link and more generally to resolve backlogs of clearance applications. These managers did not have a background in vetting, nor did they have any formal qualifications.

While I accept that managers will utilise a different range of skills than practitioners, it is particularly important that middle-level managers, who make decisions on day-to-day policies and procedures at the NCC, have relevant qualifications. It can also be difficult for managers to demonstrate expertise or credibility if they do not hold the same qualification deemed mandatory for others.

Appropriately qualified managers should assist with the reinforcement of the fundamental principles of security vetting within DSA.

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.

Training for new practices and systems

Since 2006 the DSA has experienced a prolonged period of significant change, covering policy, structure, systems and staffing arrangements. This period also coincided with a rapid growth in the requirement for security clearances across Australian Government agencies. One of the key areas which contributed to the unauthorised and inappropriate vetting practices in the NCC was the failure to provide appropriate training to staff as part of the change management process.

In particular, the change management process following the introduction of the DSA-ASIO link was unsatisfactory in that there was little in the way of training provided either before or after the system was introduced.

I was advised by staff at the NCC that changes to processes following the introduction of the link were generally developed via informal meetings between team leaders and this was then passed on to their respective teams by word of mouth. However, no one has been able to provide me with a satisfactory account of how an absent staff-member was to keep abreast of the changes discussed. I was also advised that minutes of meetings, which included discussions on change, began to be formally documented and distributed to staff some time in late 2009 or early 2010. The minutes presented to me reflected a varying degree of quality and frequency, and would not adequately replace formal instructions.

It is not surprising that inconsistencies between teams were common. Without a formal mechanism for managing changes or recording procedures, staff would ‘compare notes’ and settle on a preferred interpretation. This was characterised by one APS staff member as ‘Chinese whispers’.

One long serving APS staff member stated under oath:

> … there’s different teams doing similar jobs. Because one area has used a workaround such as [Green Street or using city name for street name] doesn’t mean that the other team did. [Fake Street and Green Street] was raised in a meeting [in May 2011] by a couple of analysts, and obviously, I didn’t even know about it, never even heard of it.

Initially the changes agreed by Team Leaders followed consultation with the Business Technology Manager in Canberra, who according to Mr Sinfield was ultimately responsible for training staff at the NCC following the introduction of the DSA-ASIO link.

Mr Sinfield's frustration with how this was progressing was expressed in an email from him to the Business Technology Manager and Assistant Director NCC on 21 May 2009 as follows:

> This problem of having to rectify the data entry faults of the NCC operators in order to meet the meta data requirements of ASIO has been around for a long time. [The Business Technology Manager], despite my asking - then directing – that this information be passed to the NCC, this has not yet occurred.
>
> Next week, [the Business Technology Manager] is in Brisbane. He WILL take the ASIO fault documents and he will train an NCC operator or two in how to rectify these problems.

Regarding his role in providing the training, the Business Technology Manager told the inquiry 'I don't think DSA was ready. I would have preferred to have rolled out a training program first'. He said he raised this issue with Mr Sinfield who advised 'that we were ready'.

In March 2010 the responsibility for data transfer errors was transferred to the NCC. An email from the then DVO, dated 17 March 2010, to managers at the NCC advises that:

> … there is no remedial ASIO function remaining in Canberra … nor should there be any remedial ASIO work being done in the regions.
>
> For [AD NCC] to be able to manage the contract staff and have them learn the correct data entry procedures you should refer all errors back to the NCC. If we don't tell him the same errors will keep occurring.

It is my opinion there was also a fundamental shortcoming in how data integrity issues resulting from the DSA-ASIO link were resolved. For example, in many of the emails I saw, the Business Technology Manager provided technical options to NCC staff on how to resolve data transfer errors, but would defer to 'the vetters' (the system users) to decide what was the appropriate course of action to take in any particular circumstance. For whatever reason – a lack of judgement, a lack of training, a lack of understanding of what ASIO required or pressure to get clearances granted – wrong decisions were made.

While I accept that data transfer issues were at the root of the widespread development of unauthorised workarounds, it is my opinion that more adequate training and change management processes could have prevented the widespread development of unauthorised and inappropriate workarounds.

The variation in practices across the organisation reflects a lack of any recognised change-management process for policy and procedures, particularly those arising from system changes.

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.

Understanding the broader picture

Contributing to the use of these workarounds was the perception that not all data required by ASIO was necessary for security assessments. NCC staff also asserted that, as the vast majority of security assessments came back as non-prejudicial, the inaccurate data made little difference in the overall vetting process. The common belief of NCC staff was that workarounds helped speed up the vetting process and that the information required by ASIO was largely redundant.

A long time APS staff member at the NCC who was an acting Team Leader for a period and the supervisor of at least one of the *Lateline* complainants, summarised this misconception:

> Those things that had to be done, such as that 1st of January 1900 and stuff, were limitations of the system at the time. And the things that were used had no impact on, or couldn't have any impact on the ASIO assessment or the processing of the clearance.

The Training Needs Analysis at Recommendation 5 should consider the need to educate staff as to how their work fits into the broader process.

QUALITY ASSURANCE PROCESSES

A Quality Assurance (QA) process was first introduced by the DSA in 2007 as a result of the PVPI review. This was later extended to Industry Vetting Panel (IVP) cases and then to NCC cases. I am advised that a random sample of completed cases, across all levels, was regularly forwarded from the NCC to Canberra for independent review.

Due to the evidence I was provided about the unauthorised workarounds occurring, I asked staff at the NCC where in the vetting process the modified data should have been identified, including whether it should have been identified during the QA process (that is, after the clearance had been granted).

Many of the co-ord staff interviewed indicated their belief that the modified data would be identified by the analyst or delegate before the clearance was granted.

This view was supported by a senior manager in Canberra, who had previously been both DVS (responsible for QA) in 2009 and DVO (responsible for the NCC) during 2010:

> In theory it should have been picked up by the analyst. [However] to be frank and fair, their job was to analyse the person's suitability for a clearance, not whether their address was correct.

Regarding the QA process, the same senior manager stated their opinion that the QA process did not look at data-entry:

> … they were looking at, perhaps, how long it [the case] was in the NCC, and were all of the documents that should have been attached to a pack there. But no, to answer your question, looking at 7 Suspect Street [on an application] to 7 Suspect Street in PSAMS, no that was not part of the quality assurance process.

When challenged that there was nobody checking the quality of the data entry, the manager stated:

> … the answer is no, but would we know that that data was not great, I would have to say yes that we would.

This view was confirmed by Mr Roberts:

> In theory, considering grants delegates as a quality assurance mechanism is valid. In practice it failed because the delegates' focus was on compliance with policy and procedures, and the quality of interviews and assessments. No one was checking the quality of the data.

In conclusion, it is my opinion that QA, both during the vetting process and after, was inadequate in respect of data quality and integrity. I make no comment about the QA of the decision-making or other parts of the process. At interview in July 2011, Mr Sinfield indicated that inadequate resources had been devoted to QA and that it was difficult to get people to do this role:

> I can't get enough staff to do it, and staff find it a boring task and don't want anything to do with it. They don't like it at all.

It was alleged that cases selected for Quality Assurance (QA) were either cherry-picked by team-leaders, or pre-identified for special treatment. I have come to the conclusion that this allegation is not supported. The claim was made without clear explanation about how it occurred or who was responsible. The allegation was disputed by managers at both the NCC and in Canberra, who explained how cases were randomly selected.

The process of Quality Assurance at the NCC requires improvement. The quality of vetting at the AGSVA should be subject to a formal quality management system.

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

STAFF MANAGEMENT

While not the direct subject of this inquiry, it has been difficult to untangle the allegations of inappropriate vetting practices from the accusations of bullying and harassment at the NCC, as well as poor management in general. The report would be incomplete without some observations in this area.

Two independent investigations commissioned by Defence were conducted at the NCC in 2010. The first concentrated on specific allegations of bullying and harassment and the second on systemic management issues at the NCC. During the course of this inquiry it became clear that there had been management shortcomings at both the NCC and the DSA.

Management oversight of the NCC

Despite a brief to the ASV in 2009 titled 'Preparing the AGSVA Workforce' describing the NCC as 'the most critical function to enable AGSVA business to continue', evidence given to this

inquiry was that staff at the NCC believed they received little direct attention from senior management in Canberra, until after the *Lateline* report.

This was disputed by Mr Roberts, who stated he visited the NCC twice in 2009 and three times in 2010 (in response to workplace complaints) and by Mr Sinfield, who indicated he visited the NCC a couple of times a year. Mr Roberts also requested me to highlight the attention the NCC received from the then DVO relating to new accommodation, OHS issues and a message sent to NCC staff following the Brisbane floods. I acknowledge these important activities but suggest that they do not, in themselves, demonstrate sufficient management oversight of the core business of the NCC.

A review of travel records from the previous two DVOs, covering the period from 2008 until early 2011 indicated the DVO for 2008 and 2009 travelled to the NCC only three times but the DVO from February 2010 until April 2011 travelled to the NCC monthly, apart from June, July and December 2010. The latter DVO further noted that to mitigate the lack of onsite visits, there were 'many daily phone calls … at least one per day'.

The absence of consistent oversight by senior managers from Canberra arguably left the Assistant Directors NCC to manage the problems at the NCC on their own. Additionally, the Brisbane-based managers were required to travel and at least one of the managers appears to have spent much of their time in 2009 and 2010 travelling to Canberra, at times on a fortnightly basis.

I note that the recommendations of the earlier Brennan and Trent reviews both highlighted the need to ensure that the NCC was managed at the appropriate level by an officer with relevant skills.

I had considered making an explicit recommendation on the need to review management oversight of the DSA and NCC but note that the current *Review of the Processes and Management Arrangements Supporting Australian Government Security Vetting* (see page 49) has within its terms of reference an explicit requirement to comment and make recommendations on the 'level and appropriateness of management oversight'. Although I have not made a specific recommendation about this, I would expect that any reporting of the implementation of Defence's response to this inquiry's recommendation would also include their progress in this area too.

Responses to previous reports

In October 2010, following the Brennan investigations into bullying and harassment and systemic management issues at the NCC, the various recommendations were combined into a single remediation plan by the then DVO. While the DSA have not been able to provide a signed copy of the document, I have been advised that the NCC Remediation Plan was accepted by the Deputy Secretary Intelligence and Security on the basis of a verbal brief provided by the CSO and the then DVO. The remediation plan contains 26 recommendations, covering 6 key areas:

- NCC Management Team
- Recruitment
- Training
- Team Building/Cultural Change
- Performance Management strategies
- Infrastructure.

During the course of the inquiry I have been advised that the recommendations in the NCC Remediation Plan have been met. However, when these recommendations were explored further, particularly at interview with relevant senior managers, it appears this was not the case for all recommendations.

Contractual arrangements

While the use of contract staff as an alternate to APS staff is a matter for Defence, I believe it is appropriate to comment on the staffing arrangements in place at the DSA. In the Australian Public Service the use of contract staff may be appropriate in certain situations, for reasons of effectiveness or efficiency, particularly to deal with short term surges in workload or to provide specialist skills for a particular task.

I was advised repeatedly by middle managers and one senior manager that use of a contracting arrangement at the NCC was not primarily for efficiency or effectiveness. The perception was that the reason for the contract workforce at the NCC was that the DSA could not employ additional staff as public servants because of a cap on additional staff. While it was recognised that extra staff were required, and that Defence had funds to support this, I was advised that a contracting arrangement was used so that no additional full time equivalent staff numbers would appear to be engaged.

Mr Roberts advised me, however, that this perception was incorrect and that the use of contract staff was primarily to allow trained APS staff to conduct analytical work while contractors did more of the administrative and data entry tasks, and in expectation that these lower level tasks would not be required following the introduction of epack2 and PSAMS2.

In any event, the use of contract staff presented particular management challenges. The terms of the contract between Defence and CML necessitated a complex flow of communication. Contractors were tasked by APS staff however they were required to raise workplace issues through their contract Team Leader. Administrative issues, such as timesheets, approval for breaks and absences and so on, were raised directly with the contract Team Leader. The contract Team Leader, who in 2009/2010 was employed by Recruitment@Top, would subsequently liaise with CML management by phone.

Mr Roberts advised:

> Management of its workforce was a Recruitment@Top responsibility … Defence set contract key performance indicators with CareersMultiList, not with individual contractors. CareersMuliList/Recruitment@Top set key performance indicators for their staff, which in hindsight may have contributed to a number of issues discussed in the draft report

When asked for an opinion on the effectiveness of the management arrangements, the DVO in 2010 stated:

> [As manager of vetting operations] I was giving half the people the story, and expecting half the people to work in a certain way… I didn't have any care, oversight or management in how the rest of the [NCC] organisation acted.

The co-location of APS and contractors together at the NCC also caused problems due to their vastly different employment conditions. This created a 'them and us' culture. For example, APS

were free to participate in social functions, such as birthday morning teas. I was advised that, apart from rare exceptions, contractors could only join the APS staff in morning tea if they were willing to forfeit pay for the lost time and had approval from their contract supervisor.

The DVO in 2010 told the inquiry:

> The inherent HR issues that someone is sitting next to someone, or can see terms and conditions of your employment are different. If you attend morning tea you don't get paid, or you're not invited to morning tea because you're not a part of that group, and you sit there smelling the sausage rolls.

I am advised that the CML contract was originally drafted with performance measured by keystroke. This inherently rewarded speed over accuracy. As the DVO in 2010 said, 'if you pay someone by keystroke, you're going to work fast, not efficiently and not correctly'. The contract was later changed from keystroke to a different measure of output, however the inability of APS staff to performance-manage contractors, and the contract's incentive for quantity over quality was described as an ongoing problem.

While the use of contact staff is a matter for Defence, I will note that the arrangements in the contract with CML resulted in a workforce that could not be appropriately managed by APS staff. If the DSA continues to use contractors it should review its arrangements.

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.

Focus on output

Many of the people I interviewed both at the NCC and at DSA in Canberra, described their perception of a culture where quantity prevailed over quality and statistics were more important than staff. They explained that this had a detrimental effect on staff morale and the quality of their work.

One senior DSA manager wrote in 2008:

> It quickly became clear to me that the pure, single focus of management in [Vetting Branch] was outputs – figures, statistics, backlog levels etc. and the need to 'manage up'. There was absolutely no focus on the people in the organisation.

Although the allegations in relation to bullying and harassment were not upheld in the 2010 Brennan investigation, the reports indicated the level of dissatisfaction among staff at the NCC was high. This could impact not only on productivity, but could also present a personnel security concern. A number of staff, at both the NCC and the DSA, suggested that a review of staff turnover and exit surveys would provide insight into the culture that prevails at the DSA. While I have not investigated turnover or absenteeism as part of this inquiry, this is one of the recommendations of the NCC Remediation Plan.

As described previously, the DSA policy dictates that any application with incomplete information is to be referred back to the applicant, either by completing a cover sheet and

returning the pack or by contacting the applicant by email or phone to find the information. When asked why staff used the workarounds rather than the correct process, they generally indicated it was due to the pressure to complete cases. Documentation provided during the course of the inquiry indicated that 'reject statistics' were reviewed on a weekly basis in 2009. While it is not unreasonable that this occurred, I note that it appears to have been a source of stress for staff.

At interview, the Assistant Director NCC at the time indicated that the sheer number of errors was the reason why the documented process did not occur:

> And the numbers of those that came up [data transfer errors], we couldn't stop the process and phone the vettees because we were getting two to three hundred a day.

I was also advised that a significant proportion of cases were identified as high priority or urgent which required shorter timeframes for turnaround. In these cases PSAMS was annotated with 'Do Not Reject' or words to that effect. This annotation was added by managers in the NCC at the direction of managers in Canberra, and seemingly removed a staff member's discretion to reject applications with incomplete information. While this may not have been the intention, the increased pressure appears to have contributed to staff resorting to workarounds in lieu of the correct process. Audit by IGD staff revealed at least 651 applications with the 'Do Not Reject' annotation since 1 January 2009.

Quite aside from the pressure to complete high priority cases within benchmarks, many staff indicated that the only time they received praise was if their statistics were deemed satisfactory irrespective of quality. A senior manager when the DSA-ASIO link was established indicated his impressions that 'the only game in town was productivity. … I was judged solely on my ability to push clearances through the system'.

One particular example of an allegation of excessive output requirement deserves closer examination. On the *Lateline* program Ms Weightman complained that she was pressured to complete the data entry for 50 Top Secret applications in one day, when most staff indicated that it was reasonable to complete 10-20 applications per day.

Management at all levels of the DSA advised me that Ms Weightman's assertion could not be true and informed me that it would not be possible to complete 50 packs in one day. I was also advised explicitly that Ms Weightman had never handled Top Secret applications.

The IGD audit confirmed Ms Weightman assertion that she had completed the data entry for the 50 Top Secret packs in one day. It remains unclear why she was instructed to complete so many in one day.

Ms Weightman suggested that due to the pressure to complete the 50 packs, which were all ePacks, there were likely to have been many data transfer errors. The audit did reveal that the person who was then responsible for data transfer errors modified the data on at least 17 of the cases processed that day on PSAMS.

It is worth noting that the pressure to complete security clearances has not disappeared since the establishment of AGSVA. Some staff at the NCC indicated that it was public knowledge that the number of cases that would need to be completed had been 'underestimated by 200 per cent'. When questioned at interview, Mr Sinfield said the Attorney General's Department had used

2007/2008 figures to calculate requirements for AGSVA but by 2009 there had been a 'paradigm shift' in the numbers of clearances required in Government. He also noted that they had expected the PSAMS Refresh Project to be completed before AGSVA was established, which would have provided the productivity gains to achieve targets. In September 2011 Mr Sinfield advised me that the experience to date was that demand is actually 20-25% greater than estimated.

Given the role of the significant and ongoing pressure in vetting over recent years, both for Defence and now for Australian government, and the need for improved systems to achieve efficient and accurate processes, I recommend a review of staffing numbers and the prioritisation of the implementation of PSAMS to deliver efficiencies in processing.

I was advised by Mr Roberts in September 2011 that the interface problems between ePack2 and PSAMS will not be fully fixed until the introduction of the upgraded PSAMS in July 2012. These problems will continue to place pressure on vetting staff.

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.

CHANGE MANAGEMENT FOR EPACK2

Given the pace and extent of change in DSA systems and processes it was critical that any implementation plans should adequately address change management issues. As noted above, the project governance arrangements for the introduction of the DSA-ASIO link did not include a dedicated change manager. Although the *Lateline* allegations related to practices that occurred prior to the implementation of ePack2, I believe that it is useful to look at the implementation of ePack2 to see whether improvements have been made.

I am advised that the oversight of the implementation of ePack2 was managed by the same team that had responsibility for the significant task of planning for and implementing the transition of the Vetting Branch to the AGSVA. This arrangement does not seem to have been fully effective.

In the early stages of the inquiry, I was informed by the DSA that the data issues in ePack had been resolved when ePack2 was introduced in September 2010 and therefore workarounds were no longer required. However, once I began interviewing staff at the NCC, it became apparent this was not the case. We subsequently became aware of and requested a copy of an email titled 'URGENT : ASV Directive' sent by Mr Sinfield to the AGSVA management team on 23 May 2011, stating:

> I am directing that until further notice, **no change** is to be made to data entered into packs by vettees, and no additional data is to be added to their information after the pack is electronically submitted by them. This includes codification of data so that it can be accepted by other agencies such as ASIO.

This email, which was released one week after the *Lateline* report aired, seems to indicate that there were ongoing concerns about whether workarounds were still being used by NCC staff at that time, that is, following the introduction of ePack2 and the establishment of AGSVA.

A further directive was sent by Mr Sinfield by email on 14 June 2011, titled 'Approved OPS Instructions' which referenced the email above and noted:

> The attached Ops Instructions have been developed to provide the appropriate management controls as outlined at the reference and are approved for use from 14 June 2011:
> - OPS 016 – Entering data into PSAMS for electronic ASIO check requests; and
> - OPS 017 – E-Pack Data Collection – Data Entry Protocols.
>
> These Ops Instructions are to be complied with from now on. Directors are to follow up this direction to confirm it is being complied with.
>
> **Note that only AGSVA APS staff are to undertake data entry into either the e-pack or PSAMS under these Ops Instructions.**

At interview, the Business Technology Manager stated that ePack2's initial list of errors numbered in the thousands. He described the rollout as 'rough' and stated:

> I didn't think it was ready to be rolled-out. I didn't think it was a production-ready system, in the sense that it wasn't particularly stable at the … original rollout date. There were fields that just didn't behave correctly. There's a wide range of issues, and it just was not a particularly pretty system at that point in time. I can't remember the exact numbers, but we'll have it documented somewhere, but it was something like, I think about 1300 to 1500 defects listed in it, which is a lot for a system that's going into a production phase.

Mr Sinfield advised the inquiry that he was aware of the unresolved system issues, but assessed the risk was manageable and approved the production release of the system in September 2010. He said he discussed this decision with Mr Roberts and that the project board had cleared this to go ahead.

> Now we knew that there were, that there would be some problems with the system, they warned me about that, and it was my decision, and I spoke with Frank [Roberts] and said that this is not 100%, but it will do the job, and it will, people will be able to use it.
>
> I was told it had been tested. I understood it had been tested, and I knew that there were so many tier 1 errors and tier 2 errors and things like that. But I was assured that the majority of these would not cause a problem in regards to people using the system.

Mr Roberts advised me that:

> … the [AGSVA] had no real option other than to accept a less-than-perfect solution in September 2010 as the Agency would not have been able to cope with the anticipated volume of paper-based applications. Another factor was the assessment that the [AGSVA] could manage the inadequacies of ePack2 while they were being fixed

One example of a system error cited by a current contractor at the NCC, who was going through the process of having her clearance upgraded at the time of the *Lateline* allegations, was that when entering data on ePack2 her date of citizenship could not be the same as her date of birth.

When she relayed this problem to the AGSVA Client Service Centre she was told to change her date of citizenship to the following month. This caused the person some concern as she believed she was providing false information on an official document. The contractor went on to explain that when she raised this concern to her team leader she was told it was 'just the machine' and not to worry about it. Nevertheless, it did continue to concern her, enough to raise it both with Mr Roberts when he visited the NCC after the *Lateline* report and to this inquiry.

During the course of the inquiry it became apparent that this was a known error in ePack2 that has since been resolved (August 2011). While the issue has been resolved, I am concerned that during the course of the interviews I conducted at the NCC, staff were not aware of the formal process for managing errors and until June 2011 there were no documented processes for dealing with this error. I also note that if the explanation provided to this contractor did nothing to allay her of concerns about the validity of the DSA processes, other applicants from the broader community would have similar concerns and this could affect confidence in the integrity of system.

As late as August 2011, Defence still held the view that the majority of the workarounds were alleviated by the introduction of ePack2 in September 2010. However this does not appear to be supported by audit data that I requested and was provided by IGD. For example, the one instance of 'Fake Street' being entered in lieu of a missing street occurred on 12 April 2011. Also, there were many instances of the suburb or city being used in place of a missing street up until 25 May 2011, two days after Mr Sinfield's email was sent. The IGD audit report further indicates that none of these streets were subsequently changed. This therefore means that the modification of data was occurring after the creation of AGSVA.

On 31 August 2011 my office received an email from Mr Roberts acknowledging that there were a significant number of workarounds in place following the introduction of ePack2 and that they had not been agreed by ASIO.

I understand that the DSA is currently working with ASIO to resolve this issue. I support this approach.

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.

Part 5 Data integrity and ASIO assessments

ASIO'S DATA REQUIREMENTS

One of the more serious allegations from the *Lateline* complainants was that as a result of the modification of data in PSAMS, the ASIO security assessments were not valid.

On 9 August 2011 Mr Frank Roberts provided a written statement to the inquiry. In his statement, Mr Roberts asserted that workarounds were used to deal with situations where the data required by ASIO was not available, and where the analyst assessed that the change involved would have little or no bearing on the overall security vetting process. It is not clear to me on what basis an analyst would have made this assessment.

It is my opinion that the staff at the DSA have consistently demonstrated limited awareness of the importance of ASIO data requirements for a security assessment. Indeed, the staff member with the greatest level of interaction with ASIO, the former DSA Business Technology Manager, stated:

> It's never been clear to me what information is actually used for the checks in ASIO… It's never been clear exactly what their checking entails.

As noted previously, Mr Roberts also advised that the workarounds called for missing data to be obtained from the vettee at a later time if possible, inserted into the pack and PSAMS once obtained and, if warranted, passed on to ASIO.

The inquiry has not found evidence to support the claim that missing data was subsequently passed to ASIO on a consistent basis. One of the cases my staff reviewed (see Appendix A) demonstrated that manufactured data persists throughout the entire process, including referral to ASIO. As for DSA's assertion that ASIO would recognise placeholders such as Green Street, Fake Street and so on, and then accommodate a correction from DSA, ASIO stated:

> Because the Defence described workarounds were not known or agreed to by ASIO, ASIO has not been in a position to know that false information was being sent and therefore needed to be 'corrected', either subsequent to or during the security assessment process. When ASIO receives information subsequent to the security assessment, or during the security assessment process, ASIO regards this information as additional information. ASIO is not aware of a process whereby false information is sent to ASIO by Defence and then Defence subsequently advises that the original information is false and proves specifically corrected information.

As outlined in the *Australian Government Personnel Security Protocol*, a security assessment by ASIO is a mandatory requirement for all clearances from Negative Vetting 1 and higher. However, it is only one part of the vetting process:

> The ASIO Security Assessment is not a substitute for evaluation of the clearance subject's suitability for access to national security classified information.
>
> ASIO Security Assessments provide further information and advice on national security issues to assist in determining whether to grant, continue, deny, revoke or vary a proposed or existing security clearance.

In light of statements by senior Defence management in the early stages of this inquiry that ASIO had approved the workarounds in place at the NCC, I asked ASIO to forward relevant documentation and to answer a number of specific questions including:

- Was ASIO aware of the workarounds and were they documented?
- Were there any workarounds in place following the introduction of ePack2 and the creation of AGSVA?
- How might the workarounds have affected the outcome of the security assessment?
- Was ASIO informed by DSA once missing data had been obtained and if so, what follow up action was taken?

Subsequent advice from ASIO was that, apart from the use of 01/01/1900 in certain limited circumstances:

> … ASIO does not now and has not previously agreed to such workarounds.
> … ASIO's position now, as in the past, remains that full and accurate information is required by ASIO to undertake its security assessment role.

Furthermore, ASIO stated that because the described workarounds were not known or agreed to by ASIO, ASIO was not in a position to know that modified information was being sent and therefore that it needed to be 'corrected'.

While evidence from both Defence and ASIO indicate that from time to time staff at the NCC provided ASIO with additional data (both in response to requests from ASIO for missing information and when additional data became available) I did not see evidence of the NCC advising ASIO that original information provided was modified or that they were correcting previously supplied data. A small sample check has confirmed that at least some modified information has been retained by ASIO. The actual amount of incorrect data that may be retained by ASIO will only be known once the remediation work described in this report is complete.

Documentation reviewed by my staff confirms that, since the early stages of testing of the DSA-ASIO link in 2008, ASIO has consistently stated that data quality in mandatory fields in PSAMS is essential for their security assessment process.

All supporting information is required to be of the highest level of detail and accuracy possible. Applications for higher level clearances, such as Top Secret Positive Vetting, have more mandatory information fields than lower level clearances.

ASIO understands that data may not be available for every field. Where this is the case, that the information is genuinely not available, they require that the information be noted as unobtainable and an explanatory comment included.

Advice from ASIO is that the impact of many of the workarounds described is 'potentially significant'.

THE INTEGRITY OF THE VETTING PROCESS

There is little doubt that the integrity of the data that has been passed from the DSA to ASIO during the period 2008 until approximately 31 August 2011 (when ASV withdrew OPS 16/17

and banned the use of workarounds) has been undermined. What is difficult to characterise is the impact on the security assessment and ultimately, the vetting outcome. Initially, the practices described appear to be benign attempts to overcome limitations of the computer systems. With increasing work-pressure and a lack of understanding of ASIO's requirements, the practice of modifying data within the NCC became common and wide-ranging.

I have established that modified data entered ASIO and persists today. Defence staff suggested that the fact that the vast majority of ASIO security assessments are returned as non-prejudicial, means that there is inherently a very low risk that the modification of data by NCC staff would have had any effect on the ASIO security assessment or the overall result of the vetting process.

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 described below (see page 48) should identify whether any cases exist.

I was advised by some staff at the NCC that while modified data was sent to ASIO for the security assessment process, this would not have affected the actual security clearance decision because analysts were working from the hard copy pack as submitted by the applicant. While this may have been the case with the original ePack, following the release of ePack2 there were some situations where modified data could make its way to the printed copy on the PSF.

Prior to the release of ePack2, applicants were instructed to print their pack once submitted and return the whole document to the NCC. With ePack2, applicants were instructed only to return the pages that required signature, although I am advised that they often returned the whole pack. Where an applicant returned the whole pack, this was placed on the PSF. If an applicant did not return the whole pack, NCC printed a copy of the pack. If the data in ePack2 was subsequently modified, via an NCC staff member resetting the applicant's password, and the pack was printed out after this time, the PSF could include modified data. The other situation where modified data could appear on the PSF, and this was observed by my staff during a review of a sample of files, was where the data was modified in PSAMS and then used to populate the ePack for a subsequent clearance action, such as a re-evaluation or upgrade of clearance.

Part 6 **Remediation**

Initially, Defence proposed auditing and re-doing clearances associated with the three complainants. I advised that, in my view, this would not focus on the correct areas. The use of workarounds was widespread, undocumented and practised by both APS and contract staff. It would therefore not be sensible to select cases based on any particular staff member or contractor.

It was also suggested that all ASIO security assessments since 2008 should be redone. While this process may provide some level of certainty that the subsequent assessments are valid, I would be concerned that this could divert resources away from ongoing security assessments and clearance processes and cause significant delays. The end-result could perversely be an increased risk to national security.

Remedial action is underway. The AGSVA 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.

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

For existing clearances, re-evaluation presents an opportunity to cleanse existing data. The data is presented to applicants who are required to certify that it has been checked. In the absence of any knowledge that the data could have been changed, most applicants probably pay cursory attention to this check. A more thorough process would improve data integrity.

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.

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 ePack2 where it seems likely that it will not be possible to identify the missing or inaccurate information. As mentioned above, AGSVA is limiting access to this function and the implementation of Recommendation 13 will cleanse the data in the longer term.

Mr Roberts has also addressed the issue of reviewing clearances in instances where the assessing officer and grant delegate is the same person. He has advised that a team has been tasked to validate security clearance data of concern to identify such instances for NV Level 1 clearances and above with a view to reviewing the validity of decisions made.

Part 7 **Further DSA reviews**

At the time of drafting this report two separate relevant reviews are underway in the DSA.

In April 2011, prior to the *Lateline* allegations, the DSA commissioned the AGSVA Organisational Structure and Business Process Review, conducted by Beca Consultants Pty Ltd.

In August 2011, in response to the preliminary findings of my inquiry, as well as in response to their own analysis, the Deputy Secretary of Intelligence and Security commissioned the Review of the Processes and Management Arrangements Supporting Australian Government Security Vetting.

The key tasks of this review are to:

- examine the existing supporting processes and the management arrangements in place to ensure that they are applied consistently across the AGSVA, and are repeatable and auditable
- make recommendations where appropriate to revise or improve AGSVA processes and management arrangements
- where possible, progressively pass these recommendations to the AGSVA for action as early as possible
- examine the progress with implementing the NCC Remediation Plan to confirm the response is comprehensive and appropriately implemented, and whether further interventions are required in light of events since the plan was developed
- make recommendations on the staffing model, the levels and appropriateness of management oversight at the respective vetting locations and the merits or otherwise of the existing geographic dispersal of AGSVA vetting centres
- consider whether the current linkages, arrangements and procedures that exist between the AGSVA and supporting external agencies (ASIO, AFP and others) are adequate, and are functioning on a clear, mutually understood basis.

This review, which is headed by an experienced SES Band 1 officer, Mr Frank Colley from the Defence Imagery and Geospatial Organisation and supported by a team of five, will report to the Deputy Secretary weekly, with a major progress report by 30 September 2011 and concluded no later than 31 October 2011. The review will consider the work already completed and underway by Beca Pty Ltd on the suitability of the AGSVA's processes and management arrangements.

My staff have been liaising closely with Mr Colley and his team to provide ongoing input into their review.

Part 8 Personal responsibility and accountability

GENERAL COMMENTS

In this inquiry I have focussed on:

- whether the allegation made on *Lateline* were true
- whether there were any other inappropriate practices
- systemic causes and contributing factors
- recommendations for improvement.

I have found that the inadequate management arrangements at a number of levels were a contributing cause of the problems encountered at the NCC.

In the report I have named only two individuals: Mr Frank Roberts, Chief Security Officer (an SES Band 2 position), and Mr Peter Sinfield, Assistant Secretary Vetting (an SES Band 1 Officer). I provided both Mr Roberts and Mr Sinfield with my preliminary views in this inquiry and offered them the opportunity to comment. Mr Roberts was concerned that the fact that only he and Mr Sinfield were named suggested that the report perhaps diminished the responsibility that non-SES staff had for the oversight and governance of the security vetting process.

My reason for naming Mr Roberts and Mr Sinfield was that their identities were, in any event, readily ascertainable from a number of public documents. I have not concluded that they were solely responsible for the management shortcomings but note, however, that as senior executive officers they hold particular positions of leadership that carry significant responsibilities in terms of accountability.

In his response to my preliminary views, Mr Sinfield submitted that the failings in the NCC were caused in part by 'the failure of the trust and responsibility I placed in my managers at subordinate levels in the organisation'.

Mr Sinfield commented:

> … it did not occur to me to ask junior staff if they were following process, it was assumed. I relied on 2-3 levels below me to report on the status of their work and accepted that my supervisors and managers would let me know if there were concerns. I believe that I encourage a workplace of openness and commitment, and I believe that most people would find it easy to give me feedback. Not once was I told by my managers that these inappropriate vetting practices were going on.

and

> Given the significant workload that was dealt with within the Vetting Branch and the Australian Government Security Vetting Agency, and considering the nature of our junior APS and contracted workforce at the National Co-ordination Centre, I had relied on [the relevant EL level staff] to capably and professionally manage the vetting system in that office. I was regularly assured though reporting channels that all systems and processed [*sic*] were being followed. I believe there was a lack of management oversight by middle

> management and the executive manager responsible for the location and what has proven to be misleading communications between them and my office.

Mr Roberts also commented that none of the inappropriate practices were ever brought to his attention.

Mr Roberts suggested that, if true, the allegations also reveal a failure by APS officers involved to act in accordance the APS and Defence values and the APS Code of Conduct, either by violating endorsed policy as alleged or not reporting it when it was observed. He wrote 'The absence of any comment to this effect suggests that the draft report appears to undervalue the notion of individual responsibility and accountability'. He also referred to a particular practice by NCC staff as 'as much a reflection on their personal professionalism as anything else'. Mr Roberts concluded that the 'draft report does not adequately reflect the obligation of responsible EL1 and 2 managers to exercise their management responsibilities and of individuals in the NCC to exercise their personal responsibility to "comply with law, policy, code of conduct and values"'.

Both Mr Roberts and Mr Sinfield express concern that where I quote staff concerns about the practices of 'senior managers' or 'management' (for example, where staff advised me of their perceptions of pressure to disregard security concerns) I do not clearly identify who was alleged to be involved.

I recognise that regional staff have a different view of who comprises 'management' or 'senior management' and that for some it could include, for example, team leaders at the APS5 level while staff in Canberra might reserve the term for senior executives. I have focussed on identifying systemic issues rather than trying to identify lapses in individual responsibility and accountability because, in my view, in circumstances where lapses are widespread that is a more productive way of identifying root causes and proposing improvements.

When assessing the contributing factors I was concerned to reflect the perceptions of staff because that is what drives their behaviours. I have not tried to ascertain which particular middle manager or supervisor was responsible for particular advice to staff or to identify who was to 'blame' for bad advice. If middle-management at the NCC applied pressure for output that seemed to be largely as a result of factors over which they had little control.

BREACH OF DUTY OR MISCONDUCT

The IGIS Act requires me to consider whether the action taken by any officer amounts to 'a breach of duty or misconduct'.

Section 17(10) of the Act states:

> Where the Inspector-General forms the opinion that there is evidence that a person who is a member of an agency has been guilty of a breach of duty or of misconduct and that the evidence is of sufficient weight to justify the Inspector-General doing so, the Inspector-General shall bring the evidence to the notice of:
> (a) in a case where the person is the head of an agency – the responsible minister; or
> (b) in any other case – the head of that agency.

When considering the actions of individual officers involved in data entry, analysis or decision-making, it is disappointing that inappropriate practices were followed, but I have received credible evidence that these staff:

- believed they were following directions from supervisors (however defined)
- felt that they were under pressure of increasing output
- were operating without adequate documentation or training
- were trying hard to maintain throughput with challenging IT systems.

I have not found evidence that the behaviour of these individuals amounted to a breach of duty or misconduct.

Similarly, supervisors, team leaders and executive level managers were faced with the same challenges and work pressures that were largely outside of their control. They did not always demonstrate the level of judgement that would be expected at this level but I have concluded that all actions relating to vetting practices – however misguided – were generally taken in good faith. There may also have been a failure to effectively escalate matters but there is no evidence that they deliberately provided false information or concealed information from management in Canberra.

I have noted above that SES officers have particular responsibilities and accountabilities as leaders. This includes the responsibility to provide assurance that organisations are following correct practices and procedures. Both Mr Roberts and Mr Sinfield have accepted a certain level of responsibility but both too have emphasised that they relied on advice (or lack of advice) from their sub-ordinates. In my view, while it may be appropriate to rely on advice to some extent, this does not diminish their individual personal responsibility or accountability. SES 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.

Both Mr Roberts and Mr Sinfield have commented that these events took place in a particularly difficult environment and that the NCC represented but part of a broad range of responsibilities and challenges. I recognise the genuine efforts made by both to manage multiple complex projects and to ensure that changes were implemented and that new systems could support the processes and achieve efficiencies. They were not supported well by the IT change program. I also note that both acted in good faith at all times.

While I have found that a significant contributing factor to these problems was lack of management oversight I have decided that there is no evidence of sufficient weight that any person was guilty of a breach of duty or of misconduct to justify referral to the Secretary of the Department of Defence.

Appendix A – **Modification of data**

1. Filling gaps in dates

Higher-level clearances rely on a reviewable chronology of an applicant's life as part of the assessment, particularly in areas such as address and employment. Any gaps in the chronology would ordinarily trigger a series of questions by vetting staff to resolve the gap. This was reflected in the business rules for the vetting information systems which would reject any gap in chronology of greater than one month.

One of the workarounds advised by NCC staff was practice of 'stretching dates' to fill gaps. This involved changing the end date of one period to a later date and the start date of the subsequent period to an earlier date. A common example provided was to close the gap when an applicant transitioned from high-school to university. The end date of high school would be changed from November to December and the start date of university would be changed from February to January. This would adjust the gap to less than a month which would allow the ASIO request to be sent. We were advised of a further example where there was a gap in address where a military member proceeds on posting and does not have a new address until some months later, possibly after a holiday and time to find suitable accommodation in the new location.

Several staff at the NCC admitted to filling gaps in this way for the transition from high school to university. Even the Business Technology Manager indicated they believed this was acceptable practice. Two other APS staff members stated they also used the practice of filling gaps, but only ever in the case of addresses for military members who were obviously moving to a new address on transfer. Others stated they filled gaps wherever they arose; in address, employment and education fields.

A variation on the practice described by a number of NCC staff, both APS and contractors, was to fill a significant gap in employment. In this case, staff would create an entry for 'unemployed' to fill the gap and use the applicant's residential address at the time. It is surmised that the origin of this workaround was that the staff first confirmed with the applicant that they had been unemployed for the period, but those we interviewed did not state this is what was required and the files reviewed did not indicate contact with the applicant.

One of the *Lateline* complainants admitted to both filling gaps by 'stretching dates' and using 'unemployed'. When asked in which circumstances they would use which method, they answered:

> There was never any definitive instructions saying 'this was the proper process'… The supervisor would make a judgement call on it. … It was an either/or thing.

The complainant in question insisted that their Team Leader at the time advised them to fill gaps in this way (as well as a number of other workarounds described on the *Lateline* program). Nevertheless, when their Team Leader was asked at interview if he had heard of these workarounds or whether he had instructed staff to use them he responded 'that would not be a practice I would have told them to do'. The Team Leader also stated that he would not use this practice (stretching dates) for a gap in education, but that he might do it in one particular circumstance where a gap in address lined up perfectly with extended overseas travel.

The only document we have found that identifies the use of 'unemployed' to fill a gap is an email from the Recruitment@Top team leader to an APS Team Leader, 'Areas to look out for!' It advises:

> Employment – Dates can overlap, however, if their [sic] is a gap of greater than 1 month then you will need to fill the gap'/s with Unemployed & use the residential address the Vettee was using at the time.

ASIO have advised that filling gaps in this way is of particular concern to them as it obfuscated the fact there was a gap, which prevented them (and the DSA) from exploring what the applicant may have been doing during the period.

2. Resolving overlaps in dates

Similar to filling gaps in dates, vetting information systems do not accept an application where dates in a chronology overlap. In these instances the staff member would adjust the date in one of the entries to fix the continuity of the chronology. There did not appear to be a consistent or documented rule for guiding which date was adjusted.

3. Using 1/1/1900 (or similar) for missing dates

The use of 1/1/1900 has been cited by the DSA as an accepted workaround that is known and approved by ASIO. The origin of this workaround appears to have been during the testing of the transfer of electronic data for the DSA-ASIO link. According to the Business Technology Manager, if '1/1/1900' is entered into PSAMS it will be converted to 'unknown' by ASIO.

ASIO acknowledges that the use of 01/01/1900 was known and agreed to for cases where the real date of birth was not known. This was accepted because a qualitative remark, such as 'unknown', could not be used in the numerical data field by ASIO. However, for the date of birth for the applicant, spouse or parents, ASIO has always required that the correct date of birth be later determined.

Indeed, an internal ASIO email dated 26 March 2008 revealed that:

> Testing has discovered that DSA have elected (without consultation with ASIO) to make use of the date 01/01/1900 in situations such as –
> - Mandatory fields where they do not have the information
> - Optional fields where their processing has unintentionally inserted this date (e.g. Sibling Death).

Interviews with staff at the NCC revealed many variations about when they believed it was appropriate to use 1/1/1900, not limited to dates of birth. Depending on the staff member questioned, it was used for:

- any missing birth dates
- *only* for birth date for an estranged parent or spouse
- *only* for the deceased date for a relative overseas
- *only* for the date-of-arrival in Australia for a parent born overseas
- *only* for the deceased date of a parent.

There was also variations described to us by NCC staff whereby 1/1/1900 could only be used when the applicant confirmed the information was unknown (and an explanation given why), or whereby it could be assumed the date is unknown and used whenever the information was missing.

Two other dates were also used by NCC staff to indicate an unknown date. One manager cited the use of 1/1/1901, and one staff member used 1/1/2000 until he was told to use 1/1/1900.

Another variation was to use 1/1/year, when only the year had been provided. Again, the application of this workaround varied depending on who was asked. It was used:

- *only* for birth date of a parent (where the year was ascertained from the applicant's birth certificate)
- *only* for deceased date of a parent
- dates of overseas travel
- dates when employment, education or address commenced and ceased.

4. Creating other dates

In some cases, a number of NCC staff described a process whereby a likely date would be inferred from other information in the application. One example given was by Ms Janice Weightman, who claimed that her Team Leader demonstrated to her how to pick feasible dates of birth for an applicant's children based on the ages of the parents. Similarly, birth dates of relatives or dates of death were also occasionally created.

A variation on this was for dates of foreign contacts. Applicants are required to disclose significant contact with foreign nationals, particularly foreign officials. As applicants often do not recall the specific date of contact, some DSA staff advised they would pick a date the applicant was travelling overseas as it was common for contact with foreign officials to occur on these occasions.

5. Adding street names

Address details are mandatory for several classes of information, including current and historical residential addresses for applicants, current addresses for relatives, addresses of educational institutions and employers. The full address was required, including street, suburb, state and postcode.

There were many examples of applicants supplying partial addresses. The most common example was not providing a street name for a school, university, employer or for a previous residential address.

Once again the process that should have been followed was to chase up the missing information from the applicant. There was no document provided by the DSA during the course of the inquiry that provided for anything different, however we were given a copy of an email to Team Leaders in the NCC titled 'PSAMS data entry'. This email includes a short list of 'must do's' and states: 'The street field under all addresses must always be completed and never left blank'. While this advice does not suggest that the process should not include contacting the applicant, it certainly seems that resolving the problem of a missing street was open to interpretation as we were advised of several different variations in how it might be resolved. These included:

- Fake Street, Green Street, Brown Street, Unknown Street or Not Specified Street
- School Street, School Road and Unknown Street for educational facilities
- use Google to pick a street in the identified suburb
- use the identified suburb or city as the street name, for example, Brisbane Street, Brisbane, Runaway Bay Street, Runaway Bay.

One APS staff member admitted to extensively use 'Green Street' and an audit of PSAMS was requested of IGD to verify this information. The audit subsequently revealed that during the period 1 January 2009 to 31 May 2011 there were 64 instances of Green Street entered by this person. Of note, the staff member admitted at interview that it was of some concern to her that when these clearance holders reviewed their information at the next clearance process that they will be wondering how these fictional addresses had appeared in their data. She recognised that the data would not have been corrected later in the vetting process.

Interestingly, although Fake Street was cited as a workaround by NCC staff and was mentioned at Senate Estimates by the Chief Security Officer after the *Lateline* report aired, an audit of PSAMS revealed only a single entry which occurred in April 2011.

Again, some staff described the practice of entering a fictional street name as a placeholder, which would then be corrected following contact with the applicant. Other staff admitted the data was never revisited and this was supported by a review of a sample of files.

One particular case showed where Green Street had been used extensively was reviewed by inquiry staff. A review of the PSF showed that the applicant's original ePack included a number of previous employer addresses as 'Not Known' and a period of residential address as 'no fixed abode'. These entries were later changed in PSAMS to Green Street, by the DSA staff member who co-orded the pack. This clearance process was subsequently cancelled before it could be completed because the applicant deployed overseas.

When another clearance request was processed some months later, the applicant submitted an updated ePack. The printout on the PSF indicates multiple entries for Green Street and it appears the document was signed as accurate by the applicant with this incorrect information present. A small sample indicates that the instances of Green Street were also imported into ASIO, where they have remained.

At a later date, after the ASIO request had been sent, a small number of the occurrences of Green Street were changed by a different assessing officer to the correct street following advice from the applicant, both on PSAMS and on the PSF. However there was no evidence that ASIO had been informed. Another two entries of Green Street were removed from PSAMS and left blank, although other Green Street entries remained.

6. Creating addresses and employers

An extension of the practice of making up missing streets was to make up entire addresses and even employers. One APS staff member disclosed picking the same particular suburb (in Brisbane), wherever one was not provided. The same staff member also indicated they used 'Green Pty Ltd' for a missing employer, however an audit of PSAMS indicates this was not common practice.

7. Picking a country

For overseas travel, especially tours that included multiple countries, applicants occasionally supplied only a continent rather than a country, for example ‘Asia’ or ‘Europe’. We were advised that the correct process for these instances was for the DSA staff member to pick the first country visited and add an appropriate comment, for example ‘Contiki tour of Europe’. However, Mr Owen Laikum revealed on the *Lateline* program that he would pick any country in the continent, for example China for Asia. Another staff member also indicated this was a common practice and used China for Asia and France for Europe.

One former staff member noted that if an applicant identified Korea as a country for overseas travel and she did not know which one, she would ‘just make it up’ and enter North Korea. In June 2010, the practice was common enough to prompt ASIO to ask the DVO to alert staff at the NCC to this error to avoid it reoccurring.

During the course of the inquiry I became aware that during the early stages of testing of the DSA-ASIO link, ‘Greenland’ had been used for a missing county. At interview, the DSA Business Technology Manager advised that in early 2008, when a country was entered in PSAMS as ‘unknown’ it was automatically translated to ‘Greenland’. He explained it had been intended to resolve this workaround before the system went through to production but it had not occurred.

Appendix B – **Other alleged practices and incidents**

1. Unaudited use of ePack password reset function by NCC staff

ePack captures an applicant's information via a web page 'PSAMS on the web' and can only be submitted by an applicant once mandatory fields are completed. The submitted form is then checked by DSA staff before it is loaded to PSAMS. The applicant gains access to their ePack form via a username and password supplied by the DSA.

I was advised that DSA staff have access to a password reset function, intended to be used when an applicant loses their password. Several APS staff members described a practice of using this access to modify data in ePack when it refused to upload to PSAMS. Staff reset an applicant's password, and then logged in to ePack using the applicant's credentials. Staff characterised this practice as 'fixing formatting errors'.

A former DVO advised the inquiry that they were aware of this practice but that it should only occur with the permission of the applicant and a record of conversation placed on file. However, it was apparent from some staff interviewed at the NCC that this permission was neither sought nor documented. I understand that in the period from the start of the use of ePack2 until 23 May 2011 over half of the ePack2 submissions may have been modified in this way.

The Business Technology Manager advised that staff at the NCC had been told not to continue this practice and when he became aware of it in the original ePack he changed it to read only. We were advised that a CIOG staff member provided the access to NCC staff in ePack2 and the practice was still continuing in August 2011 when our interviews were being conducted.

Subsequent inquiries indicate that changes to ePack passwords are not captured in audit logs. Staff at IGD further advised it is possible to establish when a password was reset, but it will not be possible to identify what data was subsequently changed or by whom.

Although many of the changes might have been straightforward and sensible, the use of this practice is of significant concern in that it bypasses all security and audit controls. The range of data changed via this method appears to be unidentifiable and given it occurs at the first step of vetting process, has the potential to significantly undermine the remainder of the process. As this practice postdates the use of paper packs these changes cannot be picked up a comparison of the paper and electronic versions, particularly after the introduction of ePack2.

2. Shredding of an adverse bankruptcy check

A number of APS staff at the NCC indicated concern at an incident in July 2009 where a discretionary bankruptcy check was requested for a Secret clearance and subsequently shredded.

According to documentation provided to the inquiry, the facts of the incident are as follows:

- The assessing officer had concerns about finances in regard to an Urgent Secret clearance (the applicant advised he had defaulted on one loan and been refused another).
- On 21 July 2009 the officer requested and received approval from the Principal Security Advisor (PSA) to conduct a bankruptcy check – according to Part D of the PSM: a

bankruptcy check is not mandatory, but is able to be conducted 'where questions or concerns arise'.

- The bankruptcy check indicated the applicant had defaulted four times and employment information conflicted with what the applicant had provided. The officer assessed the case to be 'problematic'.
- On 22 July 2009 Mr Sinfield sent an email to the DSA Vetting Branch Managers for distribution, advising:

> There is a new policy directive coming out shortly which will cover the types of financial checks required for security clearances in line with PSM and DSM requirements. Until the policy is released, which will hopefully be next week or so, the following directive is to be followed by vetting staff:
>
> Bankruptcy checks are to be conducted for **Top Secret NV and PV clearances** only. Bankruptcy checks for SECRET clearances are no longer required.

- The assessing officer placed a file note dated 23 July 2009 on the applicant's PSF outlining the information of concern on the bankruptcy check and advice by her Team Leader to shred the bankruptcy check and not to proceed with questions relating to the applicant's financial history.
- The PSF was selected for Quality Assurance. The report dated 17 September 2009 instructs that further analysis of the applicant's financial situation is required and notes 'Mandatory checks should not be shredded'.
- The report was subsequently signed by then DVS and annotated with a handwritten note that further work was to be done and advising the then AD NCC that the DVO wished to speak to them about the matter.

According to another NCC staff member seated nearby, the assessing officer was angry about being told to shred the document. There was the perception that the document needed to be shredded because it was 'inconvenient' and would slow down the urgent clearance. In interview under oath in July 2011 (two years after the event), the assessing officer acknowledged the event but expressed the opinion that she was directed to shred the document because the check should not have been approved, not because the information was adverse and might slow down the process.

The relevant PSA acknowledged awareness of the case at interview, stating they 'possibly could have' been involved in the incident, but they also noted their opinion that the check should never have been approved in the first place.

Staff at the NCC alleged that the ASV had directed the document to be shredded and that the Chief Security Officer, Mr Frank Roberts, was aware of the QA report and had been angry because the check should never have been shredded. At interview, Mr Sinfield recalled the release of the email but stated he had no knowledge of the shredding of the document and had not advised anyone to do so. Mr Roberts did not recall the incident.

In conclusion, I believe in all likelihood that the direction to the assessing officer to shred the document came from their immediate supervisor and that it was in response to the email from Mr Sinfield and not due to the adverse information it contained. That said, it was not appropriate to shred the document and once the adverse information was known it should have been addressed, as occurred following the QA report. This incident has been interpreted by staff as confirming

their concerns about the integrity of their management and work practices at the time. It is unfortunate that a lack of communication and documentation allowed this interpretation to persist.

3. Officers approving their own work

A series of allegations were made in relation to the delegation to approve clearances, specifically that delegates at the NCC were approving their own assessment work negating the independent checks that result from different officers performing each function.

I was advised that policy at the DSA is that the recommending officer and approving officer must be two different and appropriately trained APS staff. This is consistent with good administrative practice.

The former DVO and DVS advised the inquiry that 'to my knowledge no one ever, ever, ever does that [sign their own clearance]'. Mr Sinfield, when asked if it was appropriate for a person to be the analyst and delegate for a clearance, responded:

> They can't be – well no, they shouldn't be… There's a set of checks and balances, and that's what it is. … There is a separate delegate and that's right across the board. That's why they have analysts and delegates as separate areas. If someone is doing the two lots then that's wrong.

Two APS staff at the NCC indicated that due to pressure to clear backlogs they were required to 'sign off' their own work and that they felt uncomfortable about this. In order to determine whether this allegation was true and the extent of the problem, I requested an audit of every occasion that a recommending officer and approving officer on PSAMS had been the same person but I was advised by IGD staff that this would be extremely difficult to provide. I subsequently requested an audit of how many times the two particular individual staff members who had made the relevant allegation had been both recommending and approving officer. The audit results supported the allegation, as demonstrated in the table below.

Level of clearance	Staff Member #1	Staff Member #2
CONFIDENTIAL	1	14
SECRET	4	12
TOP SECRET	2	4
Total	**7**	**30**

Number of times two selected staff at the NCC were both recommending and approving authority, by clearance level.

These figures indicate that an officer approving their own work occurred; however, I accept that staff at the EL2 level did not know that these practices were taking place. Although I have only examined data for two individuals I have no reason to believe that other staff would not also have been signing off their own work.

A later audit performed by Defence indicated that between November 2010 and September 2011 there were approximately 6700 instances where baseline clearances had been processed with the same person acting as assessing officer and delegate. Defence is currently investigating the practice to determine whether it compromised any clearances. This practice may be reasonable but was not documented or supported by a documented risk analysis.

Continued investigation by Defence found an additional 735 clearances in the same period across the full range of clearances where the assessing officer and the delegate were the same person. A very small sample of 20 (across 7 clearance levels) identified one case that raised concerns. The other cases in the sample were where:

- the initial vetting had been conducted by an IVP
- the transfer of a clearance was for an officer who was being transferred
- the clearance was deemed (for a baseline clearance where the checks undertaken during recruitment action were included in the process).

Although it might not be unreasonable to have a single approving officer in these circumstances, the procedures were not documented and staff did not clearly understand why the practices varied.

4. Allegations of pressure to ignore security concerns

Several long-time APS staff, both at the NCC and in Canberra, advised of pressure to disregard what they considered to be serious security concerns, particularly at the NV and PV levels. While this issue was not explored at great depth it is worthwhile noting that some staff expressed a belief that they were, at the very least, pressured into ignoring security concerns, and in extreme cases, coerced into approving clearances about which they held serious doubts.

One former APS Team Leader at the NCC told the inquiry that he often felt pressured to sign off clearances. He said if he was not comfortable in granting a clearance he would pass it to an APS6 to sign off and usually they would do so, but:

> well I felt there were some cases where I was kinda looked at 'what are you talking about stupid', you know 'there's nothing wrong with this', …'you're just being inflexible'.

The Assistant Director NCC at the time, was adamant that staff were not pressured into granting clearances, but stated his belief:

> …[staff were] just supposed to sign off what came back from IVP on the basis that they're trained and they know what they're doing. Basically, our instructions from Pete [Sinfield] were they were just supposed to have a cursory look and unless something really stood out, they were supposed to grant it.

Mr Sinfield did not agree with this assertion.

Some managers countered these allegation by stating that certain staff were 'risk averse'. However, on the face of it at least, some of the examples cited to me appeared to indicate real concerns. I note that escalation of a case when a decision-maker is uncertain is an appropriate administrative procedure. It seems that escalation was used for cases deemed 'complex', but some NCC staff members expressed to me that they had to grant clearances regardless of their concerns and without satisfactory explanation. I have not confirmed whether this actually happened.

If, as suggested by some managers, the issue was that staff did not consider the mitigating factors, this would suggest that more training is required to ensure that staff are capable and confident of making these decisions.

5. Incidents of modifying documents and disregarding some policies

Several serious allegations were also made during the course of the inquiry, concerning the modification of official documents and disregard for mandatory requirements of vetting policies.

These allegations include:

- commencing the vetting process without a correctly signed and witnessed General Consent or Official Secrecy form
- altering dates on General Consent forms to make the dates for the applicant and witness signatures match
- disregarding mandatory document requirements, for example accepting a school certificate in place of a birth certificate for an applicant born overseas
- disregarding the mandated Gold Standard for identification
- disregarding DIAC citizenship rules when making nationality determinations.

Many of these allegations would be difficult to prove except through an extensive and time consuming forensic audit. However, I am of the opinion that there were enough claims by NCC staff, both contractor and APS, to come to the conclusion that these practices did occur, even if not on a widespread basis.

In the course of the inquiry my staff reviewed 28 PSFs at the Secret and Top Secret level. The review did reveal at least one instance of a Top Secret vetting process where a school certificate was accepted in lieu of a birth certificate for an applicant born overseas. Another of the PSFs reviewed clearly indicated that a correctly signed consent form was not received until some time after the vetting process commenced.

One of the more serious allegations by one former contractor at the NCC was that they had witnessed a current APS staff member falsify a General Consent form by changing the date to ensure the date of the applicant and witness signatures matched. While this incident was denied by the accused person, at least two other APS staff (one current and one former) told the inquiry under oath that they were aware of this happening on occasion under authorisation by a PSA. I have no reason to doubt this evidence.

6. Granting provisional access without an ASIO assessment

A small number of DSA staff noted concern about the practice of the ‘provisional granting of security clearances’ without an ASIO security assessment. I am advised by Defence that, in fact, the more accurate description would be the granting of ‘provisional access’ and that this lack of clarity has caused part of the confusion.

Some staff seemed concerned that this should happen at all and another staff member advised of a concern relating to a specific ASV Directive that caused some confusion. While it is open to the DSA to take a risk-based approach in making the decision to grant access provisionally without an ASIO assessment, I do feel it appropriate to note the circumstances in relation to the directive and raise some general concerns about the documentation of ASIO security assessments.

On 28 May 2010, ASV released a directive authorising ‘staff with the necessary delegation to grant provisional access to subjects where the clearance was awaiting ASIO Assessment’ in specific circumstances outlined. It stated:

> This directive will commence on 31 May 2010 and will expire on 1 October 2010 unless cancelled sooner.

At least one APS staff member noted concern at interview in July 2011 that this was continuing after the expiry date on 1 October 2010. When I inquired into this, I was provided with an email chain that revealed that on 30 September 2010 – the day before the directive was due to expire – the Acting Assistant Director NCC had requested advice from the then DVO, as to whether the provisional 'clearances' should continue after that date. This prompted a formal response from the DVO, to all operations managers as follows:

> As the answer affects you all I thought you could all have the benefit of the response …
>
> The new AG's Protective Security Policy Framework (PSPF) which has formally replaced the PSM allows as policy, that the AGSVA can grant security clearances without the ASIO assessment. Therefore we do not need to extend the Vetting Branch Directive. However, the way in which we execute the PSPF within the AGSVA will be in accordance with the directive.

While it is clear from the email that it was intended that the practice continue, and I note that this coincided with a particularly busy period, that is the week before AGSVA was stood up, I am concerned that the email was not sent until prompted by NCC staff. I am also concerned that some nine months after the email was sent, a number of delegates at the NCC were not aware of the advice in the email and were still using a checklist that indicated the directive expired on 1 October 2010. That is, they were contravening the instructions on the form.

Additionally, after reviewing the Protective Security Policy Framework (PSPF) and other relevant documentation, I formed the opinion that, counter to the advice in this email, an ASIO security assessment *is* a mandatory check for a security clearance, and any waiver of this requirement should be properly documented.

A senior executive officer advised me in September 2011 that in his view 'the policy stating that an ASIO check is mandatory is ambiguous in the PSPF'. However Defence advised me in October 2011 that it has always understood and complied with policy that obtaining an ASIO assessment is a mandatory requirement for all clearances at NV1 or above under the PSPF.

A further allegation raised by an APS staff member at the NCC in relation to this directive was that initially there was no process to follow up on the 'provisional clearances' once the ASIO assessment had been received or even to ensure that the ASIO assessment was eventually obtained. I am informed this was later rectified, but I am concerned there was no documented process in place at the start.

In a separate but related issue, a review of a sample of PSFs from the NCC, conducted by my staff as part of this inquiry, indicated that the documentation of ASIO security assessments is poor. On the majority of the PSFs reviewed, there was nothing to indicate the ASIO assessment had been received, including the absence of even a tick in the appropriate box or a date received on the delegate checklist. This was in stark contrast to all other checks documented on the PSF.

A senior executive advised me in September 2011 that PSAMS was the record for ASIO security assessments, not the PSF, but this conflicts with other advice that PSAMS was not designed as a

record keeping database. This is confirmed by the requirement in the Defence Security Manual Edition that PSFs must contain ‘all information provided by other organisations or individuals’ including ‘the Australian Security Intelligence Organisation (ASIO) assessment’.

The incomplete record in the PSF increases the risk of mistakes being made and clearances being granted without this important mandatory check.