The Auditor-General
Audit Report No.49 2011–12
Performance Audit

Security Assessments of Individuals

Australian Security Intelligence Organisation

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81257 8

Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:
webmaster@anao.gov.au

Australian National Audit Office

Canberra ACT
25 June 2012

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Australian Security Intelligence Organisation with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit and the accompanying brochure to the Parliament. The report is titled *Security Assessments of Individuals*.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—http://www.anao.gov.au.

Yours sincerely

Ian McPhee
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **webmaster@anao.gov.au**

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team
Celine Roach
Adam Thomas
Tom Clarke

Contents

Tables

Figures

Abbreviations

AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
AIC	Australian Intelligence Community
ASIC	Aviation Security Identification Cards
ASIO	Australian Security Intelligence Organisation
BISA	Border Intelligence and Security Assessments branch
CT	Counter-terrorism
DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
DSA	Defence Security Authority
FTE	Full-time Employee
IAD	Investigative Analysis Division
ICC	Intelligence Coordination Committee
IDC	Immigration Detention Centres
IGIS	Inspector General of Intelligence and Security
IMA	Irregular Maritime Arrival
IT	Information Technology
MoU	Memorandum of Understanding
MSIC	Maritime Security Identification Cards

NHS	National Health Security
PJCIS	Parliamentary Joint Committee on Intelligence and Security
SABI	Security Assessments and Border Investigations division
SIEV	Suspected Illegal Entry Vessel
SLA	Service Level Agreement
SOP	Standard Operational Procedures
SPC	Staff Placements Committee
SRMF	Strategic Risk Management Framework
SRS	Security Referral Service
STF	Security Triaging Framework
UNHCR	United Nations High Commissioner for Refugees
VSATI	Visa Security Assessments and Travel Intelligence branch

Glossary

Adverse advice	An assessment in which ASIO recommends that a 'prescribed administrative action' be taken (cancellation of a passport, for example) or not taken (declining access to a security controlled area, for example).
Bridging visa	A temporary visa that provides for a non-citizen to remain lawful in certain circumstances where they do not hold a substantive visa.
Community detention	Community-based detention arrangements, introduced in June 2005, enable people to reside in the community without needing to be escorted. Conditions include a mandatory requirement to report regularly and reside at the address specified by the Minister for Immigration and Citizenship. Community-based detention arrangements do not give a person any lawful status in Australia, nor does it give them the rights and entitlements of a person living in the community on a visa (for example, the right to study or work).
Qualified advice	An assessment which generally means that ASIO has identified information relevant to security, but is not making a recommendation in relation to the proposed action.
Non-prejudicial advice	An assessment which means that ASIO has no security related concerns about the proposed action.

Summary and Recommendations

Summary

Introduction

1. The Australian Security Intelligence Organisation (ASIO) was established in 1949 as Australia's national security intelligence service. The agency operates under the direction of the Director-General of Security who is accountable to the Attorney-General. ASIO's role is to identify and investigate threats to security, wherever they arise, and to provide advice to protect Australia, its people and its interests.[1] ASIO's roles and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).

2. One of ASIO's key responsibilities is to provide security assessments of individuals to other Australian Government client agencies. These assessments are defined in the ASIO Act and other legislation. The main types of assessments are:

- visa security assessments—undertaken for the Department of Immigration and Citizenship (DIAC)[2];
- personnel security assessments—undertaken for the Australian Government Security Vetting Agency (AGSVA) and AGSVA-exempt agencies[3]; and
- counter-terrorism security assessments—undertaken for AusCheck[4] and the AFP.[5]

---

1 <www.asio.gov.au/About-ASIO/Overview.html> [Accessed 30 January 2012].

2 Any person applying for a visa to travel to, or remain in, Australia may have the application referred by DIAC to ASIO for a security assessment. In most visa categories, a visa may not be issued where ASIO determines the applicant to be a risk to 'security', as defined in the ASIO Act. ASIO's security intelligence investigations will from time to time determine that the holder of a valid visa presents a risk to Australia's security. In these circumstances, ASIO may make an adverse assessment and the visa will be cancelled.

3 AGSVA undertakes security clearances of employees, prospective employees or contractors on behalf of most Australian Government agencies. ASIO provides a security assessment on applicants to determine whether they pose a national security threat if allowed to access classified material.

4 AusCheck coordinates background checks and assesses the overall suitability of persons seeking identity cards that enable access to sensitive air and maritime port areas—Aviation Security Identification Cards (ASIC) and Maritime Security Identification Cards (MSIC). ASIO may recommend against issuing an ASIC or MSIC on the basis of counter terrorism security concerns.

3. In the last six years, ASIO has completed, on average, 179 847 security assessments annually.[6] The number of security assessments completed varies from year to year and between assessment types. Over this period (from 2005–06 to 2010–11), ASIO completed between:

- 34 000 and 73 000 visa security assessments annually (around 20 per cent to 40 per cent of the annual security assessment caseload);
- 18 000 and 31 000 personnel security assessments annually (around nine per cent to 16 per cent of the annual caseload); and
- 65 000 to more than 135 000 counter-terrorism security assessments annually (around 40 per cent to 66 per cent of the annual caseload).

4. Demand for security assessments and the complexity of the security assessment caseload fluctuates, driven by changes in the security environment and other factors. For example, Aviation Security Identification Card (ASIC), Maritime Security Identification Card (MSIC) and National Health Security (NHS) checks generally require counter-terrorism security assessments every two years.[7] By contrast, demand for visa security assessments is affected by factors such as changes in the movements of people, particularly those seeking to claim protection, and in Government policies in relation to such people.

5. ASIO security assessments can range from a basic check of personal details against intelligence holdings, to a complex, in-depth investigation to determine the nature and extent of an identified threat to Australia's national security. Generally speaking, while any security assessment can be complex, the more complex cases fall predominantly within the visa security assessment caseload. Cases where the identity of an individual is hard to verify, or where it is difficult to obtain and assess the necessary background information about

---

5 ASIO also provides (via the AFP) counter-terrorism security assessments for access to sensitive or dangerous goods such as explosives and radiological material (for example, ammonium nitrate, explosives and access to the Australian Nuclear Science and Technology Organisation), and to support accreditation for special events (such as the Commonwealth Heads of Government Meeting, Asia-Pacific Economic Cooperation and the Commonwealth Games).

6 ASIO's security assessments may also apply to certain applications for Australian citizenship (citizenship may not be approved where ASIO has made an adverse or qualified security assessment), and in relation to certain passports (ASIO may request on security grounds the cancellation of an Australian passport, or that an application for an Australian passport is declined. An adverse ASIO security assessment can also be grounds for the Foreign Minister to demand the surrender of a foreign travel document, such as a passport).

7 See ANAO Report No.39 2010–11 *Management of the Aviation and Maritime Security Identification Card Schemes.* NHS checks comprise a small minority (approximately 0.2 per cent) of the overall total number of checks conducted by ASIO on behalf of Auscheck.

the individual (for example, where this information, if it exists, is held overseas, or where the reliability of information may be in question) can be particularly complex.

6. The Irregular Maritime Arrivals (IMAs) component of the visa security assessment caseload is noteworthy for its complex nature. IMAs typically arrive without proper documentation and, when required, IMA-related security assessments generally entail extensive ASIO investigation. While the total number of completed security assessments has fluctuated, without a discernable trend, the complexity of the security assessment caseload has increased markedly in recent times, driven by the sharp increase in IMAs since 2009. In the six years prior to 2009, between four and seven suspected illegal entry vessels (SIEVs) arrived annually, carrying between 11 and 161 passengers and crew.[8] Table S1 shows the number of SIEV arrivals, including their passengers and crew, from 2009 to 2011.

Table S1

SIEV arrivals to Australia (2009 to 2011)

Calendar year	Number of SIEVs	Number of passengers and crew
2009	60	2726
2010	134	6555
2011	69	4565

Source: ASIO.

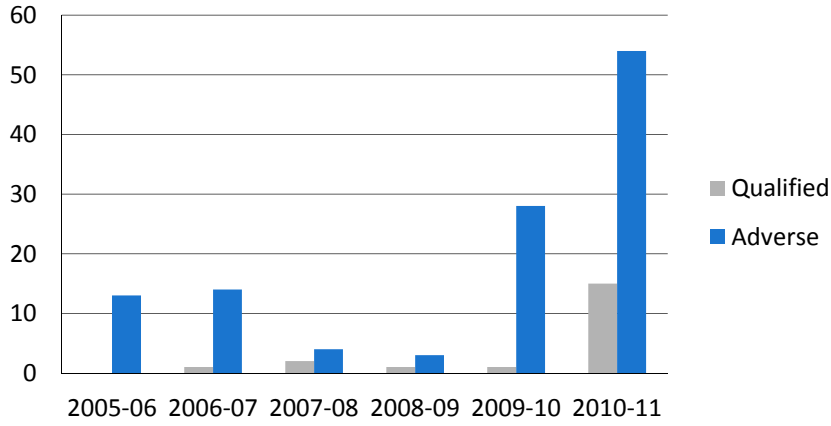
7. Upon making an assessment, ASIO may provide one of three types of advice for the client agency to take into account in relation to the individual concerned. The advice may be: non-prejudicial; or prejudicial—either qualified or adverse.[9] Reflecting the increased complexity of the cases that are being processed, the number of prejudicial assessments has more than doubled over the last six years, but remains small overall (see Figure S1).

[8] ASIO advised that not all 161 SIEV arrivals were referred to ASIO for security assessment. Crew were not referred, and at that time only adult IMAs who met the referral criteria (minority of IMAs) were referred for security assessment.

[9] Non prejudicial advice means that ASIO has no security related concerns about the action proposed in respect of the individual concerned. Qualified advice generally means that ASIO has identified information relevant to security, but is not making a recommendation in relation to the proposed action. Adverse advice means that ASIO recommends that 'prescribed administrative action' be taken (such as: declining an application for a visa, or personnel security clearance, or for ASIC or MSIC).

Figure S1

Prejudicial assessments 2005–06 to 2010–11 (number)[10]



Source: ANAO based on ASIO classified and unclassified Reports to Parliament.

8. Primarily, adverse security assessments have come from the visa security assessments stream (that includes the IMAs), and qualified security assessments from the personnel security assessments stream.

Public concerns about the security assessment process

9. Aspects of the security assessment process have attracted recent public comment. In particular, it has been noted that the time taken to complete certain security assessments, particularly for IMAs in detention, has affected the speed with which visa outcomes have been achieved for these individuals. In addition, the consequences of adverse assessments for these individuals have been the subject of public concerns. In certain IMA cases, the individual has been assessed by DIAC as meeting the definition of a 'refugee', but has also been given an adverse security assessment by ASIO. Such people are not eligible for the grant of a permanent Protection visa and, under current policy parameters, are presently ineligible for release into community detention. Unless an alternative country can be found for settlement, the individual can, in practice, remain in detention indefinitely.[11]

[10] Excludes ASIO security assessments relating to passport cancellations.

[11] ASIO noted that options for return consistent with Australia's international protection obligations (that is when it is safe to do so), review of protection obligations and third party resettlement may be available to government. However, these options are either not practical or have not been achievable to date.

Audit objective, criteria and scope

10. The objective of the audit was to assess the effectiveness of ASIO's arrangements for providing timely and soundly based security assessments of individuals to client agencies.

11. The audit assessed whether ASIO has:

- effective governance arrangements, including an appropriate risk management framework, to support the management of the security assessment process;
- a sound and timely security assessment process that is consistently applied and well supported by adequate resources; and
- appropriate client management arrangements to effectively process the security assessments of individuals.

12. The audit did not examine ASIO's broader intelligence systems and assessment capabilities or the operations of Australian Government client agencies. The ANAO used a stratified random sample of 411 cases across six security assessment categories from 2009–10 and 2010–11 to assess compliance with procedures and to better understand issues affecting the processing of the caseload. The audit also took into account previous ANAO activity[12] and other external reviews.[13]

13. In conducting this audit, the ANAO necessarily held discussions and reviewed documents which reflected matters that are sensitive from a national security and operational perspective (such as detailed information about ASIO's sources, intelligence systems and methods, or resources). In line with previous practice, these matters are not discussed in detail in this report as this would not be in the public interest. It nevertheless reflects positively on public

[12] For example: ANAO Audit Reports No.39 2010–11, *Management of the Aviation and Maritime Security Identification Card Schemes*; No.4 2010–11, *National Security Hotline*; and, No.35 2008–09, *Management of the Movement Alert List*. The ANAO also has a long-standing program of auditing visa related programs that include the following: *Management of Student Visas* (Audit Report No. 46 2010–11); *Visa Management: Working Holiday Makers* (Audit Report No. 7 2006–07) and *Onshore Compliance—Visa Overstayers and Non-Citizens Working Illegally* (Audit Report No. 2 2004–05).

[13] For example, the *Final Report* of the Joint Select Committee on Australia's Immigration Detention Network (March 2012), canvassed issues to do with security assessments, including the length of time taken to complete security assessments; the need to detain people for the duration of the assessments; and adverse assessments and the lack of opportunity for review. The report of the Inspector General of Intelligence and Security *Inquiry into allegations of inappropriate vetting practices by the Defence Security Authority and related matters* (February 2012), also involved aspects of ASIO's personnel security assessments.

administration in Australia that the *Auditor-General Act 1997* provides for performance audits of organisations such as ASIO, with appropriate reporting of their performance to the Parliament.

Overall Conclusion

14. The provision of security assessment advice of individuals to Australian Government client agencies is one of ASIO's key responsibilities. For the past six years ASIO has finalised, on average, nearly 180 000 security assessments annually in relation to people who have applied for visas, Australian Government security clearances, access to sensitive air and maritime port areas, and health security checks. The environment within which ASIO provides this service is dynamic, with demand for security assessments, and the complexity of the caseload, fluctuating substantially. In seeking to meet the changing demand for particular security assessments, and to take into account government and client agencies' policies and processing priorities, ASIO also applies an approach that gives precedence to Australia's national security considerations.

15. ASIO security assessments can range from a basic check of personal details against intelligence holdings, to a complex, in-depth investigation to determine the nature and extent of an identified threat to Australia's national security. Complex investigations can take a considerable time to complete. While any security assessment can be complex, the more complex cases fall predominantly within the visa security assessment caseload, particularly in the IMA component of this caseload.

16. ASIO's capacity to respond to changes in its security assessment operating environment was challenged in 2009–10 and 2010–11 when demand for more complex assessments increased, in line with the increase in IMA cases. A backlog of security assessments ensued and the processing times of certain security assessments, particularly for IMAs who were in mandatory detention, attracted public comment and criticism. The ANAO's sample included some cases with prolonged processing times (up to 918 days), particularly in the visa security assessments stream. For visa security assessment components that had informal time standards in place, around 51 per cent of sampled cases met expected timeframes.[14] However, personnel

[14] ASIO has informally set time standards with DIAC for the security assessment of applicants for visas in the: temporary and permanent residence, onshore protection, and offshore refugee and humanitarian visa classes. The standards range from one to six months, depending on the visa class.

security and counter-terrorism security assessments were generally processed more promptly—75 per cent of personnel security cases were processed within one day, and 90 per cent of counter-terrorism cases were processed within five days.

17. A range of factors have contributed to the time taken to process security assessments. The most influential factors identified by ASIO were the increase in the number and complexity of cases in the visa security assessments stream, and changes in Government policies and client agencies' priorities, particularly DIAC. While some of these factors were environmental, and beyond ASIO's direct control, ASIO has sought to inform Government and client agencies of the effects of particular policy approaches on the security assessment caseload. Areas of particular focus in this regard include decisions by Government and DIAC to suspend, and then subsequently, to prioritise elements of the IMA caseload. Assessment data shows that the number of pending cases has fallen from its peaks, as recent management initiatives, discussed below, have taken effect.

18. Within this context, the ANAO concluded that ASIO's arrangements for providing security assessments of individuals to client agencies are robust and, broadly, effective. The agency has a sound governance framework in place, including strategic risk management arrangements that are updated regularly. There is an effective mechanism to report to the ASIO Executive and the Government on risks that affect security assessment processes, including most recently, the emerging area of risk arising from the rapidly increasing number of security checks for immigration community detention cases.[15] However, at an operational level, there are some aspects of the security assessment regime that deserve further focus. These aspects limit assurance that the agency is making sound assessments that result in non-prejudicial advice, and that the recent initiatives implemented to reduce the IMA security assessment caseload are being managed sustainably. It is also important to address impediments to mutual accountability between ASIO and its client agencies, and that ASIO puts in place workforce planning strategies to respond to future changes in demand for security assessments.

[15] On 1 November 2011, the Inspector General of Intelligence and Security announced that she had commenced an inquiry into community detention security assessments and related matters.

Assurance that security assessments are soundly based

19. ASIO staff are well-trained and follow clearly defined procedures in conducting security assessments.[16] All 411 cases examined by the ANAO complied fully with ASIO's processes and procedures. In terms of the quality of the judgements made by ASIO assessors[17], there are quality assurance processes in place for the small proportion of security assessments that result in prejudicial advice. However, for those assessments that result in non-prejudicial advice, the quality assurance processes are not as robust and vary across assessment categories. Given that a security assessment may contribute to a client agency's decision to allow a person entry to Australia or access to sensitive information and/or locations, it would be prudent for ASIO to have in place a consistent quality assurance process to regularly validate, on a sample basis, its non-prejudicial security assessments.

Sustaining successful initiatives to improve IMA processing

20. ASIO and DIAC have worked together to streamline the IMA security assessments caseload. In particular, the introduction of a risk-based 'triaging' approach has successfully reduced the IMA backlog, and eased pressure on the overall security assessment function. However, the approach, which involves an ASIO team conducting an initial security check of IMA cases to decide whether the IMA will be referred to ASIO for a thorough security assessment, or sent back to DIAC for protection visa processing, could have been introduced in a more timely fashion. It would also be strengthened with documented guidance and a more robust IT supporting system.

Formalising relationships with key client agencies

21. ASIO has an ongoing working relationship with three key client agencies (DIAC, AGSVA, and AusCheck), and has in place a formal arrangement with one, AusCheck, which clearly articulates the responsibilities of both agencies. However, the absence of such arrangements with DIAC and AGSVA impedes the accountability of ASIO and the client agencies to each other in relation to the conduct of security assessments. Presently, there are no formally settled processing times, or service standards, for ASIO's security assessment of non-complex cases, nor any agreed arrangements for ASIO to

[16] The procedures followed by ASIO are classified. The ANAO based its analysis on the application of these procedures.

[17] The ANAO did not seek to 'second guess' the judgements arrived at by ASIO officers conducting particular security assessments.

proactively provide to client agencies regular updates on the status of complex cases—particularly those that may have lengthy processing times. At the same time, the quality of the data provided by DIAC and AGSVA, upon which ASIO depends, has frequently been poor, and required re-work, which has delayed processing. Formalising arrangements with client agencies would provide a basis for better managing mutual expectations and responsibilities in relation to these matters.

Workforce planning strategies for the security assessment areas

22. To manage the allocation of staffing resources across the whole organisation, ASIO has developed a strategic workforce plan. However, given its agency-level focus, this plan does not address the needs of individual operational areas. The security assessment areas have specialised staffing requirements that have historically proved difficult to fill. At the time of the audit, these areas were significantly under-staffed—by some 30 per cent. The agency has sought to respond to staffing shortfalls through temporary measures such as internal staffing, re-allocations and overtime. However, going forward the agency's capacity to respond, at an operational level, to future changes in the security assessment caseload would be strengthened by putting in place more long-term workforce planning strategies, including for a contingency or 'surge' capacity for this function.

Recommendations

23. Against this background, the ANAO has made four recommendations aimed at strengthening the effectiveness of ASIO's arrangements for providing timely and soundly based security assessments of individuals to client agencies. The recommendations relate to: implementing quality assurance processes for non-prejudicial assessments; sustaining the risk-based 'triaging' initiative for IMA cases; formalising agency relationships; and strengthening workforce planning strategies for the security assessment areas.

Key Findings by Chapter

Governance arrangements (Chapter 2)

24. Changes in demand for security assessments, particularly as a consequence of the sharp increase in IMAs, have had profound impacts on a number of government agencies, including ASIO. Such a dynamic environment places a premium on responsive and adaptive governance and

management arrangements. The ANAO observed that:

- ASIO's governance framework, including risk management, is robust;
- roles and responsibilities of the areas within the agency that conduct, manage and issue security assessments have been clearly documented and are well understood by relevant staff; and
- there is clear and timely reporting to the Executive and to government, where necessary, on emerging risks that affect security assessment processes and the effectiveness of mitigation strategies.

25. Operationally, there is room for improvement in two key areas: client agency relationship management and workforce planning.

26. ASIO has a current Memorandum of Understanding with AusCheck. However, there are no formal arrangements in place between ASIO and its other key client agencies, DIAC and AGSVA. ASIO has expressed a general reluctance to be 'tied-down' to specific service standards or timeframes with DIAC and AGSVA, given the complexities surrounding particular security assessments that can prolong the process.

27. The data provided by DIAC and AGSVA to ASIO has frequently been incomplete or of poor quality. For example, in relation to the ANAO's sample, 38 per cent of permanent visa referrals and 30 per cent of temporary visa referrals had incomplete mandatory information, and/or data quality issues, which required the case to be sent back to DIAC. The time taken to provide the complete information was lengthy in some cases. Similarly, ASIO advised that there have been referrals returned to AGSVA, with error codes that relate to missing mandatory information.

28. In addition, ASIO is not able to provide its client agencies with the underlying reasons as to why some complex cases are taking longer to process or specific aspects of a security assessment investigation, as the provision of substantive security information on an individual could constitute 'security advice' under the ASIO Act. Such advice is only given at the conclusion of a security assessment. These issues should be taken into account in any steps taken to formalise arrangements between ASIO and its client agencies.

29. To manage the allocation of staffing resources across the whole organisation, ASIO has developed a strategic workforce plan, which details, among other things: a scan of the current internal and external workforce environment, the challenges facing ASIO over the coming years, and ASIO's approach to these challenges. The strategic workforce plan is high level and,

given its focus, does not address the needs of individual divisions or branches. While systemic workforce shortages have been raised corporately by the security assessment branches, there is no long-term strategy in place to address these issues or to develop a contingency, or surge capacity, to respond to future changes in demand for security assessments. In practice, ASIO has found it difficult to recruit assessors to perform work on security assessments. The staffing complement of the security assessment areas has been consistently below authorised levels—in early 2012 the shortfall was around 30 per cent.

Conduct of security assessments (Chapter 3)

30. ASIO's security assessments range from relatively straightforward checks of names against data holdings to more complex investigations where an in-depth knowledge of an applicant (for a visa, for example) is obtained, and this knowledge is used to make more informed investigations, evaluations and determinations.

31. The ANAO examined a sample of 411 cases drawn from six security assessment categories.[18] The results of ANAO's analysis are very positive: all 411 cases complied with the agency's defined processes and procedures for security assessments.

32. The ANAO did not seek to 'second guess' the judgements arrived at by ASIO officers conducting particular security assessments, however, the agency's processes to assure itself as to the quality of assessments were examined.[19] Quality assurance arrangements vary across ASIO's security assessment categories. There is a robust, quality assurance system in place for all security assessments that have been issued with prejudicial advice, but quality assurance for security assessments that have been issued with non-prejudicial advice is inconsistent. For example, there is a quality assurance process to validate security assessments for IMAs, personnel security and counter-terrorism cases. However, for other visa security assessments, there is no process in place.

[18] The six categories examined were: temporary visas, permanent residence, onshore protection and offshore refugee/humanitarian, IMAs, personnel security and counter-terrorism security assessments.

[19] The ANAO also notes that the Inspector-General of Intelligence and Security provides independent assurance for the Prime Minister, senior ministers and Parliament as to whether Australia's intelligence and security agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities (see <http://www.igis.gov.au/> accessed 26 April 2012).

The Security Triaging Framework

33. Prior to April 2011, all IMAs that arrived in Australia were subject to ASIO security assessments that involved a full investigative process. Under a parallel processing arrangement, ASIO conducted its investigations of IMAs at the same time as DIAC was determining the IMA's claims to refugee status. The approach proved difficult to sustain when the number of IMAs arriving increased so markedly.

34. In late 2010, the Government made two significant decisions to streamline the security assessment process. The first was that DIAC would only refer IMAs to ASIO for security assessment who had already been accorded refugee status, or whose refugee claims could be accepted by DIAC.

35. The second decision agreed by the Government in late 2010 was to streamline the security assessment process for IMAs, to further reduce the number of IMA cases referred to ASIO for assessment. The revised risk based assessment is more closely aligned to the process applied to every other visa applicant. This process is known as the Security Triaging Framework (STF), and involves an ASIO triaging team processing the IMA referrals from DIAC that have been confirmed as meeting the definition of a 'refugee'[20] and may require a security assessment. The triaging team conducts an initial security check, based on ASIO's security indicators, and then decides whether the IMA will be referred to ASIO for a thorough security assessment, or sent back to DIAC for protection visa processing. The STF was implemented in April 2011, following riots at the Christmas Island detention centre the previous month.

36. While the Government and DIAC's responses to the STF have been positive, and security assessment and related visa backlogs within both agencies have been reduced, the ANAO identified administrative weaknesses in the triaging process. There are no documented standard operating procedures for the STF function, and the team is heavily reliant on the team leader's expertise. Further, the IT tools used by the triaging team are very basic and potentially unstable. The triaging team uses Excel spreadsheets received from DIAC, which are manually 'cleaned', copied and pasted to produce various reports prior to triaging. There is a clear risk of losing important data

[20] As a member of the international community, Australia shares responsibility for protecting refugees and resolving refugee situations. The 1951 United Nations Convention relating to the Status of Refugees states that a person is owed protection if that person is outside their country and is unable or unwilling to go back because they have a well-founded fear that they will be persecuted because of their race, religion, nationality, political opinion or membership of a particular social group.

and introducing, or retaining, errors in such a manual process. Consideration should be given, on a cost-benefit basis, to enhancing the supporting IT tools for the STF initiative.

An emerging area of risk: security checks for community detention cases

37. In October 2010, the Minister for Immigration and Citizenship announced the expansion of the existing 'residence determination' program (also known as community detention) to children and vulnerable family groups. Community-based detention arrangements were introduced in June 2005 to enable people to reside in the community without needing to be escorted. Only the Minister for Immigration and Citizenship can approve residence determination for people in immigration detention.[21]

38. DIAC and ASIO agreed to implement a streamlined security check for IMAs identified for residence determination, but who had not yet received a full security assessment in relation to the granting of a visa. At the time of the announcement, it was expected that around 900 IMAs would be moved into community detention between October/November 2010 and June 2011. Of these 900, ASIO expected to be referred around 200 cases for streamlined security checks, based on ASIO's understanding that these individuals were low-risk (adults drawn from a cohort comprising vulnerable family groups and unaccompanied minors). In an eight month period, the cumulative number of security checks increased by almost 500 per cent, from 644 cases in April 2011 to 2858 cases in December 2011. The trend is likely to continue as DIAC has now requested that all IMAs be referred to ASIO for community detention security assessments rather than the initial, smaller, low-risk cohort.

39. Initially, ASIO applied specific security indicator thresholds to its community detention assessments that were consistent with the overall low-risk nature of the expected caseload. In November 2011, ASIO appropriately revised its security assessment thresholds for community detention in light of the changing risk profile of the community detention cohort. The same threshold now applies across all IMA security assessments. This means that ASIO will issue an adverse security assessment in relation to

[21] The Minister must consider what is in the public's best interest when making, varying or revoking a residence determination under the *Migration Act 1958*. Community-based detention arrangements do not give a person any lawful status in Australia, nor do they confer the rights and entitlements of a person who holds a visa (for example, the right to study or work). The person remains, administratively, detained under migration law while living in the community. Conditions include a mandatory requirement to report regularly and reside at the address specified by the Minister.

community detention if the IMA was assessed as representing a direct or indirect risk to security.

40. ASIO advised that there have been between five and 10 cases where IMAs have been referred to ASIO for community detention security assessments despite ASIO having already issued an adverse security assessment or qualified security assessment in relation to a grant of a visa. Such persons are presently not eligible for release into community detention.

Workload and performance trends for security assessments (Chapter 4)

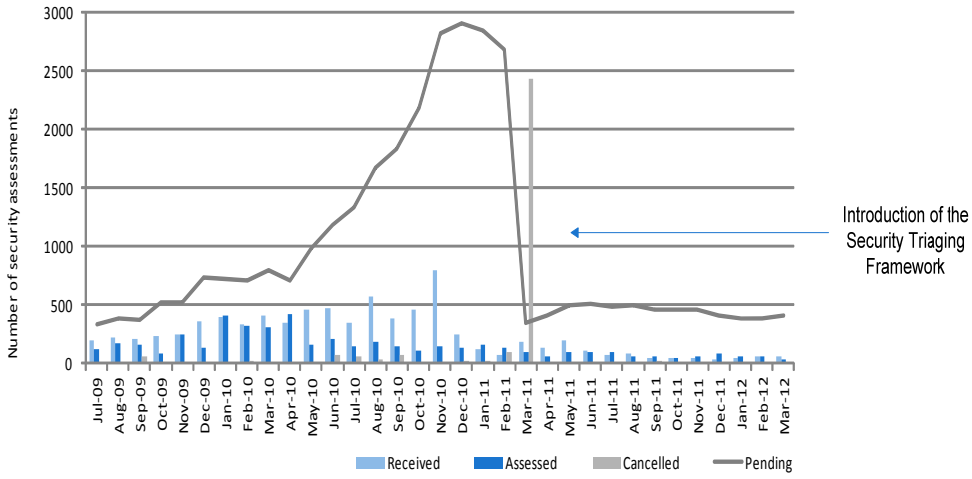
41. With the increase in IMAs stretching the processing capacity of ASIO, turnaround times for processing security assessments exceeded expected timeframes across all security assessment categories that have specified time standards. Backlogs ensued as the demand for security assessments exceeded the output capacity of ASIO staff.

42. In its public reporting, ASIO has only ever reported on the number of assessments completed. Such output measures do not give a complete picture of trends in the assessment caseload. In particular, trend data on referrals received from client agencies, cases on-hand ('pending') and processing times for key security assessment categories would provide greater insight into the management of this important function.

43. Since 2009, the trend in referrals and pending cases across the security assessment categories followed a consistent pattern, albeit with differing case numbers over specific time periods. In each category, assessment output remained fairly constant as referrals, and consequently the number of pending cases, grew rapidly over a period of months. The backlogs fell as management initiatives brought the caseload under control. For the IMA caseload in particular, the substantial decline of referrals in the first half of 2011 reflects the new intelligence-led, risk based approach being taken, including the STF (see Figure S 2).

Figure S2

IMA caseload trends (June 2009 to March 2012)



Source: ANAO analysis of ASIO data.

44. The aspect of ASIO's security assessment process that has attracted the most public comment and criticism in recent years is its timeliness. Given the importance of ASIO security assessments in progressing client agency processes, it would be reasonable to expect that ASIO and its client agencies would have formally settled on service standards or timeframes for the provision of security assessments. However, the ANAO found that in relation to:

- visa security assessments: no time standards have been formally settled between ASIO and DIAC, although informal standards have been set for some visa security assessment types;[22]
- personnel security assessments: there are also no time standards, formal or informal, settled between ASIO and AGSVA; however,
- counter-terrorism security assessments: time standards have been formally set between ASIO and AusCheck in their Memorandum of

[22] ASIO has informal agreement with DIAC on time standards for the security assessment of applicants for visas in the: temporary and permanent residence, onshore protection, and offshore refugee and humanitarian visa classes.

Understanding. In most cases, identities of these applicants are known and easily verified.

The absence of any formal arrangement on reasonable processing times limits the accountability between ASIO and its key client agencies and should be a consideration when developing formal arrangements with these agencies.

45. The ANAO's analysis of the 411 case sample showed that, for security assessment categories that had specified time standards in place, 34 per cent of cases exceeded expected timeframes. In particular, 71 per cent of security assessments for protection visas exceeded the informally agreed timeframes. Similarly, the increase in the volume and complexities of IMAs, compounded by internal staffing issues, caused prolonged processing of IMAs. These caseloads were also particularly affected by changes in Government policies and/or DIAC processing priorities. Given the complexity of such cases, it is impractical to specify an expected processing time—however, it should be possible for arrangements to be put in place for ASIO to proactively provide regular updates to client agencies on the status of such complex cases without prematurely disclosing information that could constitute security advice.

46. Conversely, for permanent visas and temporary visa cases, 65 per cent and 58 per cent of cases sampled were processed within the informally agreed timeframes. Seventy-five per cent of personnel security assessments were processed within one day, although no processing standard has been agreed for this assessment type. Ninety per cent of counter-terrorism cases were processed within the formally agreed timeframe of five days.

47. A number of factors can affect the length of time it takes to process security assessments. Some key factors identified by the ANAO from its sample include:

- quality of information/data received from referring agencies;
- the increase in the number and complexity of cases;
- changes in government policies and client agencies' priorities (such as suspending processing of certain groups and prioritising the processing of others); and
- staffing levels and backlogs.

ASIO management particularly highlighted the combined operational impact of changes in Government policies and client agency processing priorities in the visa security assessment stream.

Summary of agency response

48. The full proposed report was provided to ASIO and extracts of the proposed report were also provided to DIAC, AGSVA and Auscheck for comment. ASIO's full response to the audit is at Appendix 1. Its summary response is as follows:

> ASIO welcomes the findings of the audit report, in particular the assessment that ASIO's arrangements for providing security assessments of individuals are robust and effective. ASIO agrees with the recommendations of the report, and notes the following:
>
> - ASIO regularly assesses staffing levels across the Organisation in the context of its Strategic Risk Management Framework and intelligence priorities.
> - ASIO will continue to progress MoUs with client agencies, noting that unlike processing matters, timeframes for investigations must necessarily be indicative only.
> - In relation to regular updates, ASIO will continue to liaise with client agencies as required on these cases.
> - ASIO notes that in relation to IMA cases, quality assurance procedures are already in place to all non-prejudicial assessments.
> - ASIO notes that documented standard operating procedures exist for staff undertaking triaging in relation to IMA cases.

Recommendations

Recommendation No. 1

Paragraph 2.30

To strengthen workforce planning strategies, including for a contingency or surge capacity for the security assessment branches, the ANAO recommends that ASIO:

- periodically re-assesses staffing levels of the security assessment branches based on current and projected risks, priorities, and caseloads; and
- develops a workforce plan for the Security Assessments and Border Investigations Division.

ASIO response: *Agreed*

Recommendation No. 2

Paragraph 2.54

To strengthen working relationships, service delivery arrangements and the sharing of information with client agencies, the ANAO recommends that ASIO establishes formal arrangements with key client agencies that address operational matters including:

- ongoing liaison and problem resolution arrangements;
- reasonable processing times for non-complex cases;
- arrangements to provide regular updates on the status of complex cases; and
- data quality expectations.

ASIO response: *Agreed*

Recommendation No. 3

Paragraph 3.16

To provide greater assurance of the security assessment process in the visa security assessments stream, the ANAO recommends that ASIO institute periodic quality assurance checks (on a sample basis) for security assessments that have been issued with non-prejudicial advice.

ASIO response: *Agreed*

Recommendation No. 4

Paragraph 3.25

To better sustain the Security Triaging Framework initiative, the ANAO recommends that ASIO documents standard operating procedures for staff, and works with DIAC to enhance the supporting IT tools for the initiative.

ASIO response: *Agreed*

Audit Findings

1. Background and Context

This chapter provides an overview of ASIO and its role in providing security assessments. It also outlines the objective, scope and methodology of the audit.

The Australian Security Intelligence Organisation (ASIO)

1.1 ASIO was established in 1949 as Australia's national security intelligence service.[23] It operates under the direction of the Director-General of Security who is accountable to the Attorney-General. ASIO's role is to identify and investigate threats to security, wherever they arise, and to provide advice to protect Australia, its people and its interests.[24] ASIO's roles and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).

1.2 The ASIO Act defines security as:

> (a) The protection of, and of the people of, the Commonwealth and the several States and Territories from:
>
> - espionage;
> - sabotage;
> - politically motivated violence;
> - promotion of communal violence;
> - attacks on Australia's defence system; or
> - acts of foreign interference; whether directed from, or committed within Australia or not.
>
> (aa) the protection of Australia's territorial and border integrity from serious threats; and
>
> (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).[25]

1.3 In fulfilling its obligations to protect Australia, its people and its interests, ASIO:

- collects security intelligence through a wide range of means, including human sources and technical operations;

---

23 <www.asio.gov.au/About-ASIO/Overview.html> [Accessed 30 January 2012].

24 ibid.

25 The ASIO Act, Part I section 4.

- assesses security intelligence and provides advice, including security assessments to Government;
- investigates and responds to threats to security;
- maintains a national counter-terrorism intelligence capability; and
- provides protective security advice.[26]

Security assessments

1.4 One of ASIO's key responsibilities is the provision of security assessments of individuals to other Australian Government agencies. These assessments are defined in the ASIO Act[27], other legislation and legislative instruments.[28] Table 1.1 outlines the areas of activity where security assessments are provided by ASIO, and their enabling legislation or Government policy.

Table 1.1

Types of security assessments

Activity	Description	Enabling legislation or Government policy
Visa Security Assessments	Undertaken for the Department of Immigration and Citizenship (DIAC). Any person applying for a visa to travel to, or remain in, Australia may have their application referred to ASIO for a security assessment. In most visa categories, a visa may not be issued where ASIO determines the applicant to be a risk to 'security', as defined in the ASIO Act.(1)	*ASIO Act 1979* *Migration Act 1958*
Personnel Security Assessments	Undertaken for the Australian Government Security Vetting Agency (AGSVA). AGSVA undertakes security clearances of employees, prospective employees or contractors on behalf of most Australian Government agencies. ASIO provides a security assessment on applicants to determine whether they pose a national security threat if allowed to access classified material.(2)	ASIO Act 1979 Protective Security Policy Framework

26 ibid.

27 ibid.

28 ASIO Act 1979, *Security Assessment Determination No. 2.*

Activity	Description	Enabling legislation or Government policy
Counter-Terrorism Security Assessments	Undertaken for AusCheck and the Australian Federal Police (AFP). AusCheck coordinates background checks and assesses the overall suitability of persons seeking identity cards that enable access to sensitive air and maritime port areas—Aviation Security Identification Cards (ASIC), Maritime Security Identification Cards (MSIC) and National Health Security (NHS) checks.(3) ASIO may recommend against issuing an ASIC or MSIC on the basis of counter-terrorism security concerns. ASIO also provides (via the AFP) counter-terrorism security assessments for access to sensitive or dangerous goods such as explosives and radiological material (such as ammonium nitrate, explosives and access to the Australian Nuclear Science and Technology Organisation), and to support accreditation for special events (such as the Commonwealth Heads of Government Meeting, Asia-Pacific Economic Cooperation and the Commonwealth Games).	*ASIO Act 1979* *Aviation Transport Security Act 2004* *Maritime Transport and Offshore Facilities Security Regulations 2003* *National Health Security Act 2007*
Australian Citizenship	Undertaken for DIAC. The Minister for Immigration and Citizenship must not approve the granting of Australian citizenship where ASIO has made an adverse or qualified security assessment on the applicant.	*ASIO Act 1979* *Australian Citizenship Act 2007*
Passports	ASIO may request on security grounds the cancellation of an Australian passport, or that an application for an Australian passport is declined. An adverse ASIO security assessment can also be grounds for the Foreign Minister to demand the surrender of a foreign travel document, such as a passport.	*ASIO Act 1979* *Australian Passports Act 2005* *Foreign Passports (Law Enforcement and Security) Act 2005*

Source: ANAO using information from ASIO website.

Note 1: ASIO's security intelligence investigations will from time to time determine that the holder of a valid visa to Australia presents a risk to Australia's security. In these circumstances, ASIO may make an adverse assessment and the visa will be cancelled.

Note 2: In making the assessment, ASIO reviews any intelligence it may hold, as well as considering known security factors.

Note 3: NHS checks comprise a small minority (approximately 0.2 per cent) of the overall total number of checks conducted by ASIO on behalf of Auscheck.

1.5 A security assessment can range from a basic security check of personal details against ASIO's intelligence holdings, to an in-depth intelligence investigation to determine the nature and extent of an identified threat to

Australia's national security. Each security assessment is handled on a case-by-case basis.[29] In preparing a security assessment, ASIO is required to only consider factors that are related to 'security', as outlined in paragraph 1.2. Security assessments are not character checks, and character factors such as criminal history, dishonesty or deceit would only be relevant if they have a bearing on security considerations. Character concerns are not in themselves sufficient grounds for ASIO to make an adverse security finding.[30]

1.6 As discussed, most security assessments are undertaken at the request of another Australian Government agency (the client agency). Upon making an assessment, ASIO may provide one of three types of advice for the client agency to take into account in relation to the individual concerned (prescribed administrative action).[31] The advice may be non-prejudicial, which means that ASIO has no security related concerns about the proposed action, or prejudicial, either:

- **qualified**, which generally means that ASIO has identified information relevant to security, but is not making a recommendation in relation to the proposed action; or
- **adverse**, in which ASIO recommends that a 'prescribed administrative action' be taken (cancellation of a passport, for example), or not taken (declining access to a security controlled area, for example).[32]

1.7 The effect of an ASIO security assessment on an individual depends on the purpose for which the assessment is made and the associated legislation, regulation or policy. In some cases, decision-makers are obliged to take (or are prevented from taking) actions because of an ASIO security assessment—such as granting visas to travel to, or remain in, Australia. In all cases, the assessment is only a single component to be considered among a range of other factors—for granting access to national security information, for example. In all

---

[29] Parliamentary Joint Committee on Intelligence and Security, *Review of Administration and Expenditure No.8—ASIO Submission*, p.31.

[30] ASIO website <www.asio.gov.au/img/files/ASIOs-Security-Assessment-Function.pdf> [Accessed 20 December 2011].

[31] The legal definition of a *prescribed administrative action* is included in Appendix 2.

[32] Parliamentary Joint Committee on Intelligence and Security, *Review of Administration and Expenditure No.8—ASIO Submission*, p.31.

cases, ASIO itself is not permitted by the ASIO Act to take any administrative action.[33]

Trends in security assessments

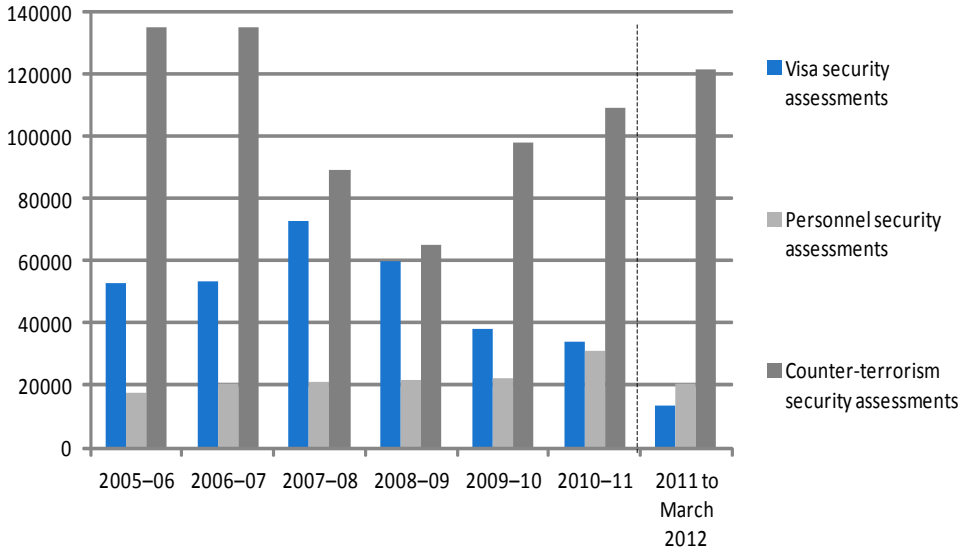
1.8 Demand for security assessments and the complexity of the security assessment caseload fluctuates, driven by changes in the security environment and other factors. For example, demand for counter-terrorism security assessments follows a distinct cycle, driven by the fact that each Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC), for which these assessments are made, expires after two or four years respectively.[34] By contrast, demand for visa security assessments is affected by factors such as changes in the movements of people, particularly those seeking to claim protection, and in Government policies in relation to such people. Figure 1.1 shows that the overall number of these security assessments made by ASIO has fluctuated, without any discernable trend.

[33] ASIO website <www.asio.gov.au/img/files/ASIOs-Security-Assessment-Function.pdf> [Accessed 20 December 2011].

[34] See ANAO Report No.39 2010–11 *Management of the Aviation and Maritime Security Identification Card Schemes*.

Figure 1.1

Total number of security assessments completed by ASIO from 2005–06 to 2011–12 (up to March 2012)

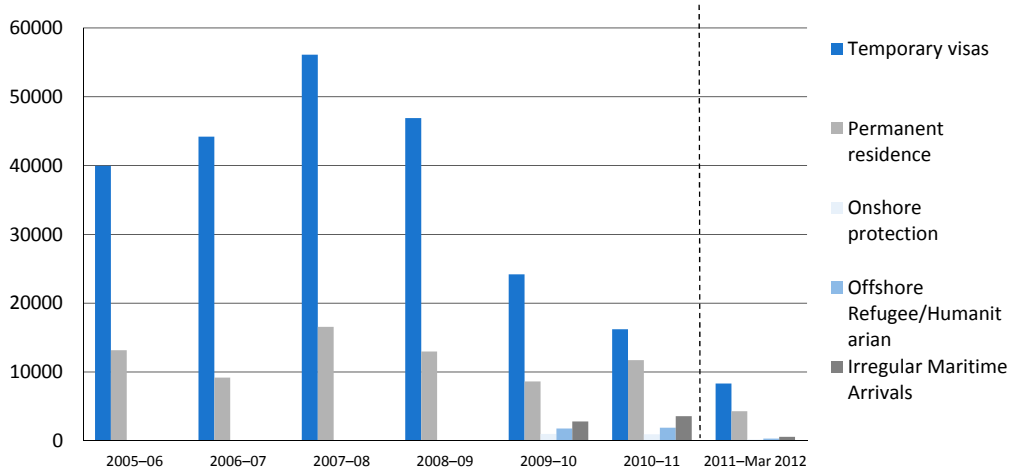


Source: ANAO based on ASIO unclassified reports to Parliament and ASIO data for July 2011 to March 2012.

1.9 Figure 1.2 below illustrates how the composition of the output of the visa security assessments stream in particular, has changed over time, with a notable decline in the generally less complex temporary entry caseload since 2007–08. However, at the same time, other, more complex, case types have increased. While the number of security assessments has fluctuated, the complexity of assessments has increased markedly in recent times, particularly in the visa security assessment stream. This complexity has placed pressure on ASIO's capacity to provide timely security assessments. The principal driver for this increased complexity has been the sharp increase in irregular maritime arrivals (IMAs) in recent years. IMAs typically arrive without proper documentation, and when required, IMA-related security assessments are generally complex, entailing more extensive ASIO investigation.

Figure 1.2

Number of visa security assessments made by ASIO July 2009 to March 2012



Source: ANAO from ASIO unclassified reports to Parliament, and ASIO data for July 2011 to March 2012.

Note: Between 2005–06 and 2008–09, IMAs were not reported separately. Since 2009–10, IMAs, onshore protection and offshore refugee/humanitarian figures have been reported separately.

1.10 In the six years prior to 2009, between four and seven suspected illegal entry vessels (SIEVs) arrived annually, carrying between 11 and 161 passengers and crew.[35] Table 1.2 shows the number of SIEV arrivals, including their passengers and crew, from 2009 to 2011.

Table 1.2

SIEV arrivals to Australia (2009 to 2011)

Calendar year	Number of SIEVs	Number of passengers and crew
2009	60	2726
2010	134	6555
2011	69	4565

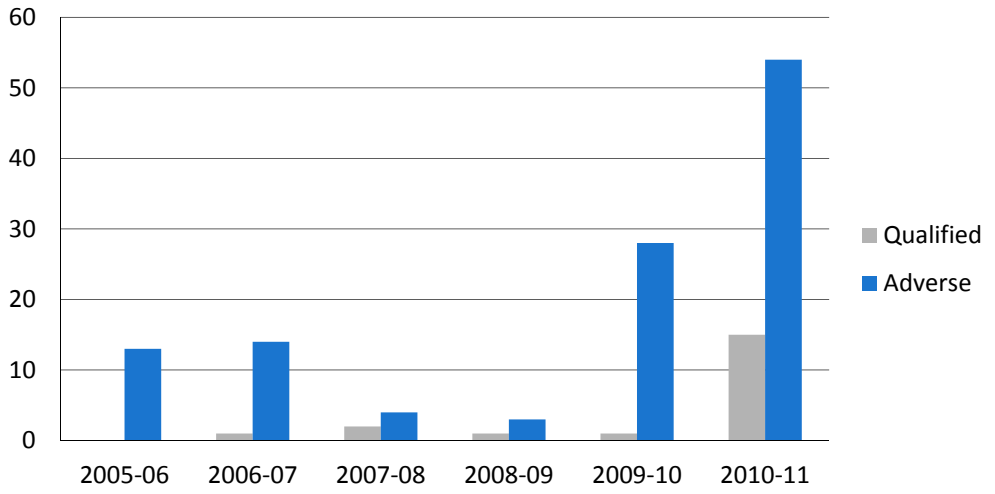
Source: ASIO.

1.11 Reflecting the increased complexity of the cases that are being assessed, the number of prejudicial assessments has more than doubled over the last six years, but remains small overall as shown in Figure 1.3.

[35] ASIO advised that not all 161 SIEV arrivals in 2003–2009 were referred to ASIO for security assessment. Crew were not referred, and at that time only adult IMAs who met referral criteria (minority of IMAs) were referred for security assessment.

Figure 1.3

Prejudicial assessments 2005–06 to 2010–11 (number)



Source: ANAO based on ASIO classified and unclassified Reports to Parliament. Excludes ASIO security assessments relating to passport cancellations.

1.12 Primarily, the adverse security assessments came from the visa security assessments stream (that includes the IMAs), and qualified security assessments from the visa security assessments and personnel security assessments stream. The majority of adverse security assessments from 2010–11 related to IMAs, and comprised around half of all adverse security assessments in the six years. The majority of qualified security assessments related to the personnel security assessment caseload, except for 2010–11, where they also came from the IMA caseload.

Public concerns about the security assessment process

1.13 Aspects of the security assessment process have attracted recent public comment, in particular the time taken to complete certain assessments, the consequences of adverse assessments for certain individuals, and reliance on government information from an IMA's country of origin.

1.14 In March 2011, a media report noted that:

> 900 people are being held in detention centres because ASIO has not completed its security checks. These 900 people have already been accepted in Australia as genuine refugees and most are being held on Christmas Island. The group makes up more than 13 per cent of Australia's total asylum seeker

> population and security delays are being blamed for overcrowding inside detention centres and millions of dollars in extra costs. They can be held indefinitely, because there is no limit on the time ASIO can take to deliver an answer on their security clearance.[36]

1.15 In addition to the length of time taken to complete some security assessments, there has been a focus on certain IMA cases, where the individual has been assessed by DIAC as meeting the definition of a 'refugee'[37] but where ASIO has also issued an adverse security assessment to DIAC. Such people are not eligible for the grant of a permanent Protection visa, and under current policy parameters, are presently not eligible for release into community detention. Unless an alternative country can be found for settlement, the individual can, in practice, remain in detention indefinitely.[38]

1.16 In a report (September 2011) to the Minister for Immigration and Citizenship, the then Commonwealth Ombudsman noted:

> … an increase in the number of people detained in an IDC for two years or more who have been found to be owed protection but have received a negative security assessment. It appears likely that the number of people in this category will continue to grow. It is noted that unless the Minister intervenes to grant a visa or approve community detention, these people will remain in a restrictive immigration detention centre indefinitely. [39]

1.17 Further, in a Parliamentary hearing of the Joint Committee on Intelligence and Security in June 2011, the Refugees, Survivors and

---

[36] ABC News, *ASIO's security check logjam revealed*, <http://www.abc.net.au/news/2011-03-01/asios-security-check-logjam-revealed/1962922> [Accessed 22 July 2011].

[37] As a member of the international community, Australia shares responsibility for protecting refugees and resolving refugee situations. The 1951 United Nations Convention relating to the Status of Refugees states that a person is owed protection if that person is outside their country and is unable or unwilling to go back because they have a well-founded fear that they will be persecuted because of their race, religion, nationality, political opinion or membership of a particular social group.

[38] ASIO advised that an adverse security assessment does not automatically result in an IMA remaining in detention indefinitely, Government has agreed that DIAC could consider removal but this must be consistent with Australia's international protection obligations. Options for return consistent with Australia's international protection obligations (that is when it is safe to do so), review of protection obligations and third country resettlement may be available to government. However, these options are either not practical or have not been achievable to date.

[39] Report by the Commonwealth and Immigration Ombudsman to the Minister for Immigration and Citizenship, *Immigration Report 652/11*, 5 September 2011, p. 2. ASIO advised that, to date, 50 of the 58 recipients of adverse security assessments since 2009 currently remain in Australian immigration detention. While the ongoing detention of these persons has focused some attention on the consequences of adverse security assessments, the action taken in relation to an IMA subsequent to ASIO making an adverse security assessment is a matter for DIAC.

Ex-detainees group commented:

> We are particularly concerned that ASIO may be relying on information that is provided by governments like the Sri Lankan Government, in our view a corrupt and human rights violating government.[40]

1.18 In March 2012, the Joint Select Committee on Australia's Immigration Detention Network released a public report that provided an overview of Australia's immigration detention network, its administration, the provision of services, impact on detainees and processes that detainees go through while in detention, including the security assessment process. The committee's report identified concerns around security assessments, in particular:

- the length of time taken to complete security assessments;
- the need to detain people for the duration of the assessments; and
- adverse assessments and the lack of opportunity for review.[41]

Financial resources

1.19 In its 2012–13 budget, ASIO's departmental annual expenses were $400.7m, up from the 2011–12 revised budget of $347.3m.[42] Funding for the provision of security assessments comprises a combination of government appropriations and fees charged by ASIO to client agencies.[43] ASIO's portfolio budget statements do not separately identify the costs associated with the conduct of security assessments. In a budget estimates hearing in February 2011, ASIO advised that:

> ASIO regularly reviews and revises the allocation of resources to Security Assessment. This may not always be a straightforward manner, as Security Assessment requires appropriate skills and expertise. For security reasons, it would be inappropriate to comment publicly on the resources dedicated to specific ASIO work.[44]

---

40 Parliamentary Joint Committee on Intelligence and Security, Canberra, 16 June 2011, p.7.

41 Joint Select Committee on Australia's Immigration Detention Network, *Final Report,* March 2012, p.158.

42 Attorney-General's Portfolio, *Portfolio Budget Statements 2012-13,* Budget Related Paper No.1.2.

43 ASIO has a fee-for-service arrangement with AusCheck for security checks undertaken for individuals applying for the ASIC and MSIC cards.

44 Senate Legal and Constitutional Affairs Committee, Answers to Questions on notice, Attorney-General's portfolio, Additional Estimates 2010–11, February 2011, Question no. 98. See also: Department of Parliamentary Services, *Australian Government spending on irregular maritime arrivals and counter-people smuggling activity,* 6 December 2011, p. 10.

1.20 While ASIO's security assessment budget is not publicly reported, it is reported within Government, including to the Department of Finance and Deregulation.

Oversight and review of ASIO

1.21 ASIO falls within the Attorney-General's portfolio and the Director-General of Security is accountable to the Attorney-General. Under section 8A(1)(a) of the ASIO Act, the Attorney-General may give the Director-General of Security written guidelines to be observed by ASIO in the performance of its functions.[45]

1.22 As part of the Australian Intelligence Community (AIC) [46], ASIO is also subject to external scrutiny, including through:

- the Inspector-General of Intelligence and Security (IGIS)—may inquire into matters concerning ASIO and investigate complaints made about ASIO from the public[47];
- the Parliamentary Joint Committee on Intelligence and Security (PJCIS)—reviews ASIO's (and other intelligence agencies') administration and expenditure. It may also conduct inquiries into matters relating to the intelligence agencies, including reviewing ASIO's use of questioning and detention powers[48]; and
- annual reports to Parliament—ASIO is the only agency in the AIC that produces an unclassified annual report.

1.23 The Security Appeals Division of the Administrative Appeals Tribunal (AAT) can also review some adverse and qualified ASIO security

---

[45] For example, in October 2007 the Attorney-General gave the Director-General of Security written guidelines in relation to obtaining, correlating, evaluating and communicating intelligence relevant to security.

[46] The Australian Intelligence Community (AIC) is an informal term used to describe the six Australian security and intelligence agencies: the Office of National Assessments (ONA); ASIO; the Australian Secret Intelligence Service (ASIS); the Defence Intelligence Organisation (DIO); the Defence Signals Directorate (DSD); and the Defence Imagery and Geospatial Organisation (DIGO).

[47] IGIS provides independent assurance for the Prime Minister, senior ministers and Parliament as to whether Australia's intelligence and security agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities. An essential function of IGIS is to report her findings at the end of each inquiry. These inquiries are conducted in private and IGIS provides her report to the responsible minister who determines what is to be released publicly.

[48] ASIO website <www.asio.gov.au/About-ASIO/Oversight-and-Accountability.html> [Accessed 22 July 2011].

assessments.[49] However, some assessments are not reviewable in the AAT if they are made in relation to a person who is not an Australian citizen; a person who is, within the meaning of the *Migration Act 1958,* the holder of a valid permanent visa; or a person who holds a special category visa or is taken by subsection 33(2) of the *Migration Act 1958* to have been granted a special purpose visa.[50]

Previous reviews of ASIO

1.24 In the past 15 years, there have been two ANAO performance audit reports that related to the security assessment process, and two performance audit reports that included ASIO (where ASIO was not the principal agency audited), as follows:

- ANAO Report no.39 2010–11 *Management of the Aviation and Maritime Security Identification Card Schemes*;
- ANAO Report no.4 2010–11 *National Security Hotline*;
- ANAO Report no.35 2008–09 *Management of the Movement Alert List*; and
- ANAO Report no.5 1998–99 *Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games*.

1.25 There have also been a number of internal reviews and enquiries on aspects of ASIO's security processes including joint reviews with DIAC. ASIO advised that it has drawn on these reviews in considering its security assessment policies, procedures, resourcing and structure.

1.26 As discussed in paragraph 1.18, in March 2012, the Joint Select Committee on Australia's Immigration Detention Network released a public report that provided an overview of Australia's immigration detention network, including ASIO's security assessment process.

1.27 In addition, in February 2012, the Minister for Defence released the report completed by IGIS into the *Inquiry into allegations of inappropriate vetting practices by the Defence Security Authority and related matters* that involved

[49] Section 54(1) of the ASIO Act provides Applications to the Tribunal, where an application may be made to the Tribunal for a review of an adverse or qualified security assessment.

[50] The ASIO Act, Part IV, Section 36. The AAT's proceedings are conducted in private and it is not bound by the rules of evidence. The AAT may inform itself on any matter in a manner that it considers appropriate. Judicial review of the process of ASIO making a security assessment is possible through the Federal and/or High Court of Australia.

aspects of ASIO's personnel security assessments. On 1 November 2011, IGIS also commenced an inquiry into community detention security assessments and related matters.

Audit approach

Audit objective, criteria and scope

1.28 The objective of the audit was to assess the effectiveness of ASIO's arrangements for providing timely and soundly-based security assessments of individuals to client agencies. The audit assessed whether ASIO has:

- effective governance arrangements, including an appropriate risk management framework, to support the management of the security assessment process;
- a sound and timely security assessment process that is consistently applied and well supported by adequate resources; and
- appropriate client management arrangements to effectively process the security assessments of individuals.

1.29 The audit did not examine ASIO's broader intelligence systems and assessment capabilities or the operations of Australian Government client agencies. The ANAO used a stratified random sample of 411 cases across six security assessment categories from 2009–10 and 2010–11 to assess compliance with procedures and to better understand issues affecting the processing of the caseload. The audit also took into account previous ANAO activity[51] and other external reviews.[52]

1.30 In conducting this audit, the ANAO necessarily held discussions and reviewed documents which reflected matters that are sensitive from a national

[51] For example: ANAO Audit Reports No.39 2010–11, *Management of the Aviation and Maritime Security Identification Card Schemes*; No.4 2010–11, *National Security Hotline*; and, No.35 2008–09, *Management of the Movement Alert List*. The ANAO also has a long-standing program of auditing visa related programs that include the following: *Management of Student Visas* (Audit Report No. 46 2010–11); *Visa Management: Working Holiday Makers* (Audit Report No. 7 2006–07) and *Onshore Compliance—Visa Overstayers and Non-Citizens Working Illegally* (Audit Report No. 2 2004–05).

[52] For example, the *Final Report* of the Joint Select Committee on Australia's Immigration Detention Network (March 2012), canvassed issues to do with security assessments, including the length of time taken to complete security assessments; the need to detain people for the duration of the assessments; and adverse assessments and the lack of opportunity for review. The report of the Inspector General of Intelligence and Security *Inquiry into allegations of inappropriate vetting practices by the Defence Security Authority and related matters* (February 2012), also involved aspects of ASIO's personnel security assessments.

security and operational perspective (such as detailed information about ASIO's sources, intelligence systems and methods, or resources). In line with previous practice, these matters are not discussed in detail in this report as this would not be in the public interest.

Audit methodology

1.31 The audit method included:

- detailed examination of a stratified random sample of 411 cases across six categories within the three broad streams of security assessments;
- review of ASIO's documentation, instructional materials and files relating to the various security assessment processes;
- interviews with ASIO officers and staff; and
- consultation with ASIO's key client agencies and external stakeholders in security assessments (DIAC, AGSVA, the Department of Foreign Affairs and Trade, AusCheck, IGIS and the AAT).

1.32 The audit was conducted in accordance with ANAO auditing standards at a cost of $350 000.

1.33 The structure of the remainder of the report is outlined in Figure 1.4.

Figure 1.4

Structure of the report

Chapter 2 **Governance Arrangements**	• Introduction • Management structure for security assessments • Risk management and reporting • Security assessment workforce and training • Client management arrangements
Chapter 3 **Conduct of Security Assessments**	• Introduction • Compliance with process and procedures • Quality assurance mechanisms • The Security Triaging Framework • Responding to an emerging area of risk: security checks for community detention cases
Chapter 4 **Workload and Performance Trends for Security Assessments**	• Introduction • Referrals received and pending cases • Processing times

2. Governance Arrangements

This chapter examines the governance arrangements that support ASIO to carry out its security assessment functions.

Introduction

2.1 Changes in demand for security assessments, particularly as a consequence of the sharp increase in IMAs, have had significant impacts on a number of government agencies, including ASIO. Such a dynamic environment places a premium on responsive and adaptive governance and management arrangements. In this context, the ANAO reviewed:

- the management structure for security assessments in ASIO;
- risk management and reporting;
- security assessment workforce, training and financial resources; and
- client management arrangements.

Management structure for security assessments

2.2 ASIO's security assessments are primarily conducted by one of ASIO's ten divisions.[53] Each ASIO division is responsible to the Director-General of Security for a defined function, ranging across, for example, investigations, surveillance, counter-espionage to security strategy.[54]

2.3 At the time of the audit, ASIO's Investigative Analysis division (IAD) was predominantly responsible for the preparation of most of its security assessment advice to client agencies.[55] Since February 2012, the newly-created Security Assessments and Border Investigations (SABI) division has primary responsibility for visa security assessments from IAD. Within SABI division, there are two branches responsible for security assessments: the Visa Security Assessments and Travel Intelligence (VSATI) branch, and the Border Intelligence and Security Assessments (BISA) branch. Table 2.1 details the specific roles and responsibilities of these two branches.

---

53 ASIO Report to Parliament 2010–11, pp. XV-XVI.

54 ibid.

55 Other divisions within ASIO are able to, and do, issue security assessments.

Table 2.1

Roles and responsibilities of the security assessment branches

Visa Security Assessments and Travel Intelligence branch
• Assesses and provides advice on applicants for permanent migration to Australia, for family or business visas. • Assesses and provides advice on applicants for temporary tourist, student and business visas, and also manages security assessments for diplomatic visas and controversial visitors. • Assesses and provides advice on applicants for protection and refugee/humanitarian visas (except for IMAs) and complex cases from temporary and permanent visas. • Manages ASIO's component of alerts within the Government's border security systems.
Border Intelligence and Security Assessments branch
• Conducts investigations and security assessments in relation to IMAs intending to enter or remain in Australia permanently. The Branch also conducts security assessments relating to individuals who are being considered by DIAC for placement in community detention. • Undertakes personnel security assessments for people who require access to national security classified information, and counter-terrorism (CT) security assessments. CT security assessments involve a basic check against ASIO's data holdings. A more complex investigation may also follow before the relevant security assessment is provided. Referrals for counter-terrorism checks are received from AusCheck and the Australian Federal Police.[56]

Source: ASIO.

2.4 The ANAO observed that the roles and responsibilities of the branches that conduct, manage and issue security assessments are appropriately documented and well understood by the relevant ASIO staff. The roles are clearly defined and are in line with ASIO's legislative and policy obligations.

Risk management and reporting

ASIO's overarching risk management framework

2.5 Risk management is an integral part of ASIO's security assessment process. The agency is required to conduct security checks and/or assessments of complex and non-complex cases against tight timeframes. Explicit risk management processes assist decision-making in such an environment.

2.6 ASIO's Executive uses a Strategic Risk Management Framework (SRMF) in managing security risks. The SRMF, which forms part of ASIO's planning and reporting processes, is a classified document that is updated

[56] AusCheck administers applications for Aviation Security Identification Cards (ASICs) and Maritime Security Identification Cards (MSICs). The AFP administers applications for people requiring licences to handle ammonium nitrate, flight crew,and people requiring access to the Australian Nuclear Science and Technology Organisation facility at Lucas Heights in Sydney.

annually. Risk treatment plans are developed by the agency's divisions/branches after the ASIO Executive has agreed on the overarching risks and risk assessments for the coming year. The risk treatment plans consider each risk in its context, the relative impact and likelihood, as well as overall risk and proposed treatments. These assessments feed into the development of the draft SRMF considered by the Executive. The progress of risk treatment plans are reviewed through various mechanisms, including direct reporting to the Executive.

2.7 Performance reports of intelligence and related activities conducted within ASIO are submitted to the Executive on a quarterly basis. The Quarterly Performance Reports identify risks that have been included in the divisions/branches' risk treatment plans. They assist ASIO's Executive in making informed decisions on actions the agency needs to take or prioritise, taking into account the risks that have been identified. They are also used to monitor risk treatments that are applied by the agency's divisions/branches.

Reporting risks relating to security assessments

2.8 Significant risks relating to security assessments should be reported to the ASIO Executive and, where necessary, to the Government to provide assurance that the risks are being appropriately managed and measures to mitigate such risks are being undertaken. The ANAO examined the former IAD's (now SABI) risk treatment plans and Quarterly Performance Reports. The Division identified and monitored risks, and recommended risk treatment plans. Progress of risk treatments were monitored and the treatment adjusted when required. For example, the risk of the increase in IMAs and staffing shortages have been included in the former IAD's risk treatment plans and Quarterly Performance Reports, which highlighted the issues to management and assisted in making decisions in relation to staffing priorities. On the basis of this information, decisions were made around the implementation of taskforces and/or the temporary transfer of staff from other areas to the BISA or VSATI branches.

2.9 In addition, matters relating to challenges encountered with the security assessment process were identified in reports to the Executive and to the Attorney-General. These included matters relating to: staffing; difficulties in meeting client agencies' expected timeframes; and the backlogs and concerns about the risks posed by the expansion of the community detention arrangements. These issues are discussed further in Chapters 3 and 4.

2.10 Overall, the ANAO considers that ASIO adopted clear and timely reporting to its Executive and to Government, where necessary, on emerging risks that affect security assessment processes. The mitigation strategies put in place to manage these risks were also monitored and reported.

Security assessment workforce and training

Workforce planning

Strategic workforce planning

2.11 ASIO has established an agency-wide workforce plan for 2011–2015 within an overarching *Human Capital Framework*.[57] This high-level plan outlines ASIO's approach to workforce planning and includes a scan of the current internal and external workforce environment, the challenges facing ASIO over the coming years, and ASIO's approach to these challenges.

2.12 ASIO's workforce planning and staffing levels are heavily influenced by the Taylor Review (2005) which recommended targets for ASIO's future staffing levels based on predictions of future intelligence priorities.[58] These staffing levels were agreed by the Government and an overall target of 1869 staff was set for the end of the 2010–11 financial year. ASIO was not able to meet this recruitment target. ASIO's forecast average staffing level for 2012–13 is 1760, unchanged from 2011–12.[59]

2.13 Implementation of the Human Capital Framework is guided by the Intelligence Coordination Committee (ICC) and the Staff Placements Committee (SPC). The ICC is the peak management committee for intelligence operations within ASIO.[60] One of its roles is allocating resources to investigative and threat priorities on a risk management basis. These priorities then filter down into the SPC which places individual staff members in vacant positions depending on the priorities agreed upon in the ICC. When operational areas identify current and future areas of concern in their workforce, these concerns are raised with their respective ICC member (for

---

[57] *ASIO Strategic Workforce Plan 2011-2015.* The ASIO Human Capital Framework 2011–13 draws existing recruiting, learning and development, performance management and HR processes into a single and aligned framework, and outlines a more analytically-driven approach to workforce planning.

[58] In 2005 Mr Allan Taylor conducted a review titled *Review of ASIO Resourcing* which assessed ASIO's capability against the post-11 September 2001 threat environment.

[59] Attorney-General's Portfolio, *Portfolio Budget Statements 2012-13,* Budget Related Paper No.1.2.

[60] The ICC has broad terms of reference that cover a range of issues surrounding intelligence operations.

example, the First Assistant Director-General) who then takes the identified concern to the committee.

Workforce planning at the operational level

2.14 Operational areas such as SABI division work with the ASIO Workforce Planning and Recruitment branch and the ICC and SPC to maintain an adequate level of staffing to perform their roles.[61] A key activity in this regard is recruiting and selecting staff with the right skills and attributes for the organisation.

Recruitment

2.15 Recruitment rounds can be either external or internal.[62] Long lead-times for external recruitment rounds mean that internal recruitment rounds, transfers, or acquiring staff through SPC decisions are often used to overcome sudden or unexpected staffing shortages. However, longer term use of internal recruitment and transfers will inevitably erode the staffing capacity of other areas of the organisation.

2.16 ASIO has found that it is often difficult to recruit for certain positions in the organisation, notably for assessors who perform some of the work for security assessments. This difficulty originates from the strong labour market in Canberra, where most of the positions are held, and the limited pool of suitably qualified people available.[63] Consequently, ASIO has had to prioritise the allocation of its pool of assessment expertise across the agency's investigative priorities. This has meant that staff vacancies in the security assessment areas have remained unfilled, a situation which has affected the time taken to process cases (see Chapter 4).

Staffing levels and demographics

2.17 Workforce planning and staffing shortages have been a recurrent issue raised in the security assessment areas' Quarterly Performance Reports for 2009–11. In January 2011, ASIO's SRMF was expanded to include the staffing concerns of both security assessment branches to better manage the increased

[61] While line areas can acquire staff through the SPC, they can also request recruitment for specific roles.

[62] External recruitment rounds take at least 18 months to complete, primarily due to the required extensive background checks, while internal recruitment is a faster process, with the entire process taking roughly two months.

[63] In October 2011, the unemployment rate in Canberra was 3.8 per cent, compared with the Australia-wide unemployment rate of 5.3 per cent. See Australian Bureau of Statistics, *Labour Force October 2011*, 10 November 2011, pp. 1 & 16.

risks associated with security assessments (including the concerns about the workforce and backlogs). Nevertheless, as of March 2012, the overall staffing level across both security assessment branches was 31 per cent under the authorised full-time equivalent (FTE) employees.[64]

2.18 The security assessment branches experienced significant staffing cuts as a result of the implementation of the recommendations from the Taylor review, with the authorised FTE being cut by over 30 per cent in November 2009. The Taylor Review recommended these reductions in 2005, when ASIO was processing much smaller security assessments caseloads than at present. In general, ASIO staff commented on the age of the Taylor Review and that its underlying assumptions no longer represent the changing risks and priorities faced by the organisation. The ANAO notes that there is a concern, both internally and with external stakeholders, that the current staffing shortages in the security assessment teams are having an adverse impact on ASIO's capacity to process assessments.

2.19 ASIO has introduced a number of measures to address staffing shortages within the security assessment branches. These measures include:

- **Taskforces**—used to address backlogs. This temporary surge capacity draws on people who have knowledge of the area and are able to provide extra capacity for a limited time.
- **Internal recruitment or transfer**—used to address workforce shortages on short notice.
- **Restructuring**—assisted in redirecting staffing resources (for example, to clear backlogs); and creating or altering positions to provide career progression for staff.
- **Overtime**—used to help clear backlogs.
- **Reviewing security assessment methodologies**—as discussed in Chapter 3, ASIO has sought to make the security assessment process more efficient by reviewing risk methodologies in order to better use available resources, and to enable ASIO to focus on investigating security threats present in the IMA stream.

[64] The number of staff assigned to the security assessment function is sensitive for operational reasons and is not disclosed in this report.

2.20 While the security assessment branches have sought to address staffing shortages and backlogs through a variety of measures, staffing shortages continue to be a significant risk to meeting the agency's business objectives.

Training for security assessment staff

2.21 Training for security assessment staff (assessors and analysts)[65] includes on-the-job training, specific training courses, and agency-wide training courses. All new staff are provided a mentor and are under close supervision when they first begin in their role. In the VSATI branch, all new assessors have a mentor for roughly six months, until they feel confident in performing the role. Likewise, staff in the BISA branch are mentored and are given closer oversight by their managers and senior analysts while under probation.

2.22 Aside from the agency-wide corporate training courses, the security assessment branches have also developed specific training courses relating to use of IT systems, analytical thinking and interviewing. Staff interviewed by the ANAO considered that the training courses they had undertaken were relevant and useful.

2.23 Further, ASIO advised that in January 2012, an internal review relating to the security assessments interview training, practices and policy was conducted. The aim was to identify any gaps and, if required, further improve guidelines or measures that are already in place. ASIO also advised that, as of March 2012, a response to the review was being drafted and that some recommendations were already being implemented by SABI division.

2.24 Overall, the ANAO considers that the training for the security assessment branches is adequate. Staff are provided on-the-job training with oversight by a mentor, have access to both specific and agency-wide training courses, and find the training relevant and useful. Attendance at all training courses is monitored.

Guidance and procedures

Standard operational procedures

2.25 Standard Operational Procedures (SOPs) provide information and guidance to ASIO staff on operational procedures and their roles and

[65] Assessors are lower classified staff that focus on less complex assessments, while analysts have a higher classification and conduct complex investigations.

responsibilities while conducting security assessments.[66] Both security assessment branches had SOPs in place, except for one directorate within the VSATI branch, which was still developing SOPs at the time of the audit.

2.26 The security assessments branches do not have a regular program of review for their SOPs. Currently, the review of SOPs is undertaken on an 'as required' basis. Some SOPs do not accurately record when they were last updated or reviewed and, at the time of the audit, some were still in draft form. There would be merit in ASIO periodically reviewing, and updating where necessary, all SOPs. Standard operational procedures should also correctly record when they were last reviewed and updated, and any SOPs currently in draft form should be finalised

Conclusion

2.27 ASIO has a sound governance framework in place, including risk management arrangements that are updated regularly. There are also effective mechanisms for reporting to the ASIO Executive and the Government on risks that affect security assessment processes. The effectiveness of the mitigation strategies put in place to manage risks were also monitored and reported.

2.28 Training for the security assessment branches is adequate. Staff are provided on-the-job training, with oversight by a mentor. They also have access to both specific and agency-wide training courses, and find the training relevant and useful. Staff are supported with a variety of useful and detailed operational guidance. However, there is no process of regular review for SOPs. In addition, many do not record when they were last updated and some are still in draft form. There would be merit in ASIO periodically reviewing, and updating if necessary, all SOPs.

2.29 To manage the allocation of staffing resources across the whole organisation, ASIO has developed a strategic workforce plan, which details, among other things: a scan of the current internal and external workforce environment, the challenges facing ASIO over the coming years, and ASIO's approach to these challenges. However, given its agency-level focus, this plan does not address the needs of individual operational areas. At the time of the audit, the security assessment areas were significantly under-staffed—by some

[66] SOP is a generic name covering a variety of operational procedural documents collected by the ANAO during the audit. The ANAO examined the security assessment branches' SOPs and undertook an analysis of ASIO's compliance to these procedures (see Chapter 3).

30 per cent. Going forward, the agency's capacity to respond, at an operational level, to future changes in the security assessment caseload would be strengthened by putting in place more specific workforce planning strategies, including for a contingency or 'surge' capacity for this function.

Recommendation No.1

2.30 To strengthen workforce planning strategies, including for a contingency or surge capacity for the security assessment branches, the ANAO recommends that ASIO:

- periodically re-assesses staffing levels of the security assessment branches based on current and projected risks, priorities, and caseloads; and
- develops a workforce plan for the Security Assessments and Border Investigations Division.

ASIO response: *Agreed.* ASIO regularly assesses staffing levels across the Organisation in the context of its Strategic Risk Management Framework and intelligence priorities.

Client management arrangements

Client agencies' understanding of the security assessment process

2.31 The security assessment process is understood, in general terms, by ASIO's client agencies. However, client agencies advised that certain aspects of the security assessment process, particularly those that may cause delay, are unclear. This lack of knowledge has been compounded by rapid turnover in key personnel at client agencies.

2.32 Historically, ASIO has been reluctant to advise client agencies about specific aspects of a security assessment investigation as it could constitute 'security advice' under the ASIO Act. Such advice is only given at the conclusion of a security assessment. Consequently, updates on the progress of individual cases have tended only to be provided when specifically requested by client agencies.

2.33 There would be merit in ASIO providing more comprehensive advice to its client agencies about the nature of the information it can provide under its legislation. Within this context, there is room for ASIO client agencies to be

provided with more information about the security assessment process on a 'need to share' basis without compromising intelligence methodologies.[67] In this regard, ASIO has initiated workshops and knowledge-sharing with some of its client agencies. The relationship with key client agencies would also be improved by ASIO proactively providing regular updates on the status of complex cases, particularly those that may have lengthy processing times.

Formal arrangements with client agencies

2.34 Typically, formal arrangements between agencies set out each party's roles and responsibilities, and define agency obligations in terms of governance, performance expectations, and reporting arrangements. They also contain agreed specifications for particular services or deliverables, including the quality measures and timeframes.[68]

2.35 ASIO has a current Memorandum of Understanding (MoU) in place with AusCheck that is reviewed on a regular basis. However, there are no formal arrangements in place between ASIO and its other key client agencies, DIAC and AGSVA.

2.36 In gathering feedback from key client agencies, the ANAO formed the view that ASIO had established generally positive working relationships in respect of its security assessment activities. It is noteworthy that the most positive relationship is with AusCheck, with which ASIO has an MoU.

2.37 As there are no formal arrangements in place with DIAC and AGSVA, accountabilities, reciprocal responsibilities and expectations are not documented and often not understood and agreed. The need for a formal arrangement between ASIO and DIAC has been raised in previous ASIO internal reviews of the security assessment process. Since 2011, ASIO has been working with DIAC to develop an umbrella agreement with draft appendices that outline the specific requirements for each security assessment category, but progress has been slow. An important factor contributing to this situation is that there is a general reluctance within ASIO to be 'tied-down' to specific timeframes with DIAC (and AGSVA), given the issues and complexities surrounding security assessments that can prolong the assessment process

[67] The Director-General of Security has stated that 'ASIO has made significant changes to its business model and culture moving from a strict policy of *need to know* toward a culture of *needing to share*. [ASIO People Capability Framework, p. 1].

[68] ANAO Audit Report No.41 2009–10, *Effective Cross-Agency Agreements*, May 2010.

(Chapter 4 analyses security assessment timeframes in detail). At the time of the audit, no formal arrangement has been initiated with AGSVA, which was established in October 2010.

2.38 Fostering a more collaborative relationship with these agencies requires a higher level of management assurance in relation to the activities and responsibilities of the service provider (ASIO), and the client agencies (DIAC and AGSVA). A formal arrangement would assist in this regard, particularly in defining and managing mutual performance expectations.

Connectivity with client agencies

Electronic transfer of data between DIAC and ASIO

2.39 The Security Referral Service (SRS) is a system that enables the electronic transfer of data (i.e. client information) relating to security assessment referrals from DIAC to ASIO.[69] If ASIO's security assessment of a client is non-prejudicial, the advice is electronically sent back to DIAC through the SRS. Prejudicial advice (both qualified and adverse) is sent back both electronically and manually to DIAC.[70]

2.40 ASIO relies on the accuracy and completeness of information sent by DIAC through the SRS to complete its assessments. At the time of the audit, SRS had not been programmed to identify situations where mandatory client information was missing or invalid. Consequently, ASIO has been receiving poor quality data, which has contributed to delays in processing security assessments.

2.41 The ANAO's analysis shows a number of cases in the audit sample (29 per cent) being referred back to DIAC (from ASIO) because of missing mandatory and/or incomplete information, primarily in the visa security assessments stream. Table 2.2 shows the results of the ANAO's analysis where missing mandatory information or further information was requested from DIAC, and the time taken for DIAC to respond to these requests.

[69] SRS was fully implemented in September 2008.

[70] Prejudicial advice is sent by ASIO to DIAC manually as back-up to the the electronic advice.

Table 2.2

Data quality and completeness in the visa security assessment stream

Visa Security Assessment type	No. of cases examined and percentage of cases that had missing mandatory information from DIAC
Permanent visas	68 cases examined. Of these, 38 per cent had missing mandatory information and were referred back to DIAC. The average time a case was with DIAC prior to being returned to ASIO was 44 days (the shortest being two days, the longest 364 days).
Temporary visas	71 cases examined. Of these, 30 per cent had missing mandatory information and were referred back to DIAC. The average time a case was with DIAC prior to being returned to ASIO was 25 days (the shortest being two days, the longest 116 days).
Onshore protection and offshore refugee or humanitarian visas	65 cases examined. Of these, 20 per cent had missing mandatory or incomplete information and were referred back to DIAC. The average time a case was with DIAC prior to being returned to ASIO was 79 days (the shortest being two days, the longest 321 days).

Source: ANAO analysis of audit sample.

2.42 Missing mandatory information included the names, addresses, place of birth, date of birth or employment of the visa applicant.[71] Other common data quality issues relate to the referral containing vague information, unexplained gaps and inconsistent information.[72] Further, the time taken by DIAC to respond with the required information was lengthy in some cases—31 per cent of visa security assessment stream (excluding IMAs) cases in the ANAO sample took more than four weeks to be re-referred with the requested information.

2.43 ASIO has tried a number of initiatives to work with DIAC to address the issue of the quality and completeness of missing mandatory information. Workshops, meetings and visits to DIAC overseas posts have been conducted to promote the importance of receiving mandatory information prior to processing security assessments.

Electronic transfer of data between AGSVA and ASIO

2.44 In December 2009, the Australian Government announced that Commonwealth security vetting processes would be centralised in the Department of Defence. The central vetting unit, known as the Australian Government Security Vetting Agency (AGSVA), conducts security vetting of

[71] Australian Government, *PIC 4002 Referral Guidelines and Helpful Hints*, May 2011.

[72] ibid.

personnel for all Commonwealth agencies (apart from certain exempt agencies). AGSVA is situated within the Defence Security Authority (DSA).

2.45 Prior to the centralisation of the Commonwealth's security vetting process, an applicant's Personal Particulars form would generally be sent to ASIO by a referring agency in hard copy form for security assessment processing. Some agencies began to send applicant information to ASIO via compact discs (in 2008). In July 2009, the electronic transfer of applicants' data became available through a fibre optic link, allowing security assessments to be completed more quickly.

2.46 However, at the time of the audit, ASIO advised that there have been ongoing problems with regards to the quality of applicants' data sent electronically by AGSVA. The agency advised that there were several hundred cases where mandatory information has been missing or incomplete. The 2011 IGIS *Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority and related matters* report stated that:

> 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.[73]

2.47 Further, ASIO advised that there have been referrals that were returned by ASIO to AGSVA because of missing mandatory information. ASIO would not process the applications further until the information required had been provided. The prevalence of errors was also mentioned in the IGIS report, which stated that:

> 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* [referred in the IGIS report as *data transfer errors*].

[73] Inspector-General of Intelligence and Security, *Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority and related matters*, December 2011, p. 20.

> I [the IGIS] was also advised that in the early days of data transfer these error reports were hundreds of pages long, with multiple errors per page.[74]

2.48 Both ASIO and AGSVA have advised that the relationship between the two agencies has improved in the period since the audit fieldwork, and completion of the IGIS report.[75] Both agencies now have a better understanding of each other's requirements and advised the ANAO that working level and executive level meetings have been established and occur regularly (monthly), or as required.

Electronic transfer of data between AusCheck and ASIO

2.49 AusCheck electronically transfers client data to ASIO in relation to counter-terrorism (CT) check applications for ASIC and MSIC cards and NHS checks. This fee-for-service arrangement is supported by a formal MoU. The agreement defines the parameters covering the transfer of client information from AusCheck to ASIO. Both agencies advised the ANAO that there are few issues with regards to data quality or missing information. In general, AusCheck's data elements in its CT check applications are compliant with ASIO data requirements.

2.50 AusCheck advised that there are incentives for the issuing body (that is, the aviation and maritime industries) to send complete applications. If the application was incomplete, they would need to resubmit the application and bear the associated costs. In addition, unlike other assessments, there are fewer fields to complete, reducing the risk of data entry errors.

Conclusion

2.51 ASIO has a current MoU with AusCheck. However, there are no formal arrangements in place between ASIO and its other key client agencies. ASIO has expressed a general reluctance to be 'tied-down' to specific service standards or timeframes with DIAC and AGSVA, given the complexities surrounding particular security assessments that can prolong the process.

2.52 ASIO relies on the accuracy and completeness of information submitted by client agencies in order to correctly conduct security assessments, and has a variety of connectivity arrangements with its key client agencies. The electronic transfer between AusCheck and ASIO works well. In contrast, the data

---

[74] ibid.

[75] Audit fieldwork and the IGIS inquiry were conducted in late 2011.

provided by DIAC and AGSVA has been incomplete or of poor quality in a high proportion of cases. In the ANAO's sample, 38 per cent of permanent visa referrals and 30 per cent of temporary visa referrals initially had missing mandatory information which required the case to be sent back to DIAC. The time taken to provide the complete information was lengthy in some cases. ASIO advised that there have been referrals returned to AGSVA because of missing mandatory information.

2.53 ASIO is not able to provide its client agencies with underlying reasons as to why some complex cases are taking longer to process or about specific aspects of a security assessment investigation. The provision of substantive security information on an individual could constitute 'security advice' under the ASIO Act, and such advice is only given at the conclusion of a security assessment. These issues should be taken into account in any steps taken to formalise arrangements between ASIO and its client agencies.

Recommendation No.2

2.54 To strengthen working relationships, service delivery arrangements and the sharing of information with client agencies, the ANAO recommends that ASIO establishes formal arrangements with key client agencies that address ongoing liaison and problem resolution arrangements, and key operational matters, including:

- reasonable processing times for non-complex cases;
- arrangements to provide regular updates on the status of complex cases; and
- data quality expectations.

ASIO response: *Agreed.* ASIO will continue to progress MoUs with client agencies. In relation to regular updates on complex cases, ASIO will continue to liaise with client agencies as required on complex cases. The nature of investigative work and its reliance on external exigencies means timeframes for investigations must necessarily be indicative only.[76]

[76] Both DIAC and AGSVA have indicated that they support the establishment of formal arrangements with ASIO.

3. Conduct of Security Assessments

This chapter examines the conduct of security assessments by ASIO and the quality assurance processes for these assessments. The Security Triaging Framework and the security checks conducted for community detention are also discussed.

Introduction

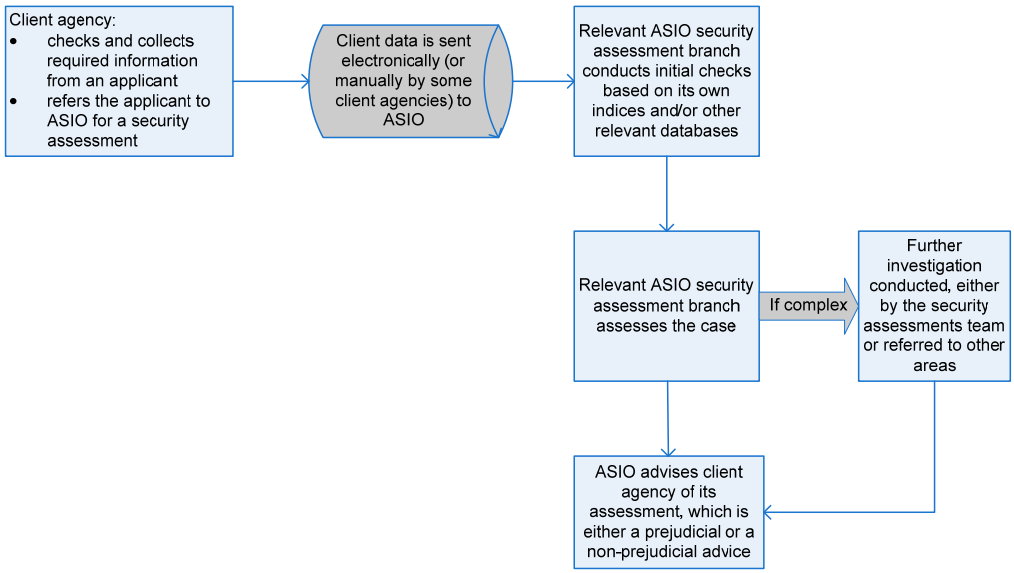
3.1 ASIO security assessments can range from a basic check of personal details against intelligence holdings, to a complex, in-depth investigation to determine the nature and extent of an identified threat to Australia's national security. While any security assessment can be complex, cases where the identity of an individual is hard to verify, or where it is difficult to obtain and assess the necessary background information about the individual (for example, where this information, if it exists, is held overseas, or where the reliability of information may be in question) can be particularly complex.

3.2 The key steps of ASIO's security assessment process for all security assessment categories are outlined in

3.3 Figure 3.1 below.

Figure 3.1

Key steps of the ASIO security assessment process



Source: ANAO analysis of ASIO data.

3.4 The ANAO examined ASIO's:

- compliance with its process and procedures;
- quality assurance mechanisms;
- Security Triaging Framework put in place to enable ASIO to focus on investigating security threats present in the IMA stream; and
- the emerging area of risk relating to security checks for community detention cases.

Compliance with process and procedures

3.5 To assess whether ASIO decision-makers had followed required processes and procedures, the ANAO examined a sample of 411 cases drawn from six security assessment categories.[77] A test program covering key aspects of the security assessment process was developed by the ANAO. Because of the sensitive nature of the process, it is described only in general terms in this report.

3.6 The ANAO did not assess ASIO's legislative compliance to Part IV of the ASIO Act[78] or the validity, appropriateness or reasons for the decisions made—this falls within the mandate of the IGIS.[79]

3.7 The results of ANAO's compliance testing were very positive: all 411 cases complied with the agency's processes and procedures. The standard of recordkeeping for the sample cases was high, supporting the integrity of the

[77] The six categories examined were: temporary visas, permanent residence, onshore protection and offshore refugee/humanitarian, IMAs, personnel security and counter-terrorism security assessments.

[78] Part IV of the *Australian Security Intelligence Organisation Act 1979* provides the legislative basis for ASIO's provision of security advice in relation to individuals.

[79] The functions of the Inspector-General in relation to ASIO are: at the request of the responsible Minister, of the Inspector-General's own motion or in response to a complaint made to the Inspector-General, to inquire into any matter that relates to: (i) the compliance by ASIO with the laws of the Commonwealth and of the States and Territories; or (ii) the compliance by ASIO with directions or guidelines given to ASIO by the responsible Minister; (iii) the propriety of particular activities of ASIO; or (iv) the effectiveness and appropriateness of the procedures of ASIO relating to the legality or propriety of the activities of ASIO; or act or practice of ASIO that is or may be inconsistent with or contrary to any human right, that constitutes or may constitute discrimination, or that is or may be unlawful under the *Age Discrimination Act 2004,* the *Disability Discrimination Act 1992,* the *Racial Discrimination Act 1975* or the *Sex Discrimination Act 1984,* being an act or practice referred to the Inspector-General by the Australian Human Rights Commission.

security assessment process. The results of the ANAO's analysis are outlined in Table 3.1 below.

Table 3.1

ANAO compliance testing results

Compliance test	Compliance with criteria	ANAO comment
Initial check for completeness of information received from the client agency	✓	**Fully compliant** Initial checks for the completeness of information received from client agencies are conducted across all security assessment categories.
Followed ASIO process specific to the security assessment category	✓	**Fully compliant.** All examined cases adhered to ASIO's defined process.
Key documentation on file	✓	**Fully compliant.** Key documents supporting the decision making process were on file across all security assessment categories. For complex and prejudicial cases, the documentation behind decisions was extensive.
Record of decisions on file	✓	**Fully compliant.** Records of decisions were kept on files across all security assessment categories.
Reason for decision has been documented	✓	**Fully compliant.** Reasons for decisions had been documented, particularly for those cases that had adverse or qualified assessments. Similarly, the reasons for decisions for non-prejudicial assessments follow the checks that led to the final advice.

Source: ANAO analysis.

Quality assurance mechanisms

3.8 ASIO's security assessment process is heavily reliant on the assessor's and analyst's judgement. A prejudicial assessment, whether qualified or adverse, can have a profound impact on a person's job, access to information, ability to travel to, or remain in, Australia. Conversely, a non-prejudicial assessment may contribute to a client agency's decision to allow a person entry to Australia or access to sensitive information and/or locations. In either case, it is important that ASIO has arrangements in place that provide assurance as to the appropriateness of its assessments.

3.9 Quality assurance is an integral part of any business process. It is a confirmation that a task, or parts of it, were accomplished in accordance with the standards set by the organisation. In ASIO, quality assurance of security assessments entails a senior ASIO officer approving or confirming a junior assessor's or analyst's judgement in the issuance of a security advice.

3.10 Quality assurance arrangements vary across ASIO's security assessment categories. For example, there is a robust quality assurance system in place for all security assessments that have been issued with prejudicial advice, that is, either qualified or adverse. These assessments are examined by higher level ASIO officers, including legal specialists and senior management.

3.11 However, the quality assurance of security assessments that have been issued with non-prejudicial advice is inconsistent.[80] For IMAs, personnel and counter-terrorism security assessments, a quality assurance process is undertaken for assessments that resulted in a non-prejudicial advice. All non-prejudicial assessments of IMAs are reviewed and approved by a senior officer. For personnel and counter-terrorism security assessments, senior officer approval is required to provide a non-prejudicial assessment in any case where security indicators are present. However, in the visa security assessments stream (other than IMAs), there is no regular, consistent quality assurance process for assessments that resulted in non-prejudicial advice, with ASIO relying on the assessor's/analyst's judgement.

3.12 ASIO advised that assessors/analysts who conduct security assessments and issue non-prejudicial advice are extensively trained, closely monitored when they are new on the job, and are free to ask their superiors when in doubt of any aspect of the process. ANAO's observations of assessors and of the application of the assessment process broadly support this view. However, given that a security assessment may contribute to a client agency's decision to allow a person entry to Australia or access to sensitive information and/or locations, it would be prudent for ASIO to have in place a consistent quality assurance process to periodically validate, on a sample basis, its non-prejudicial security assessments. Such assurance would be particularly beneficial in relation to individuals who do not have administrative appeal rights, such as visa applicants (see paragraph 1.23).

[80] Non-prejudicial advice means that ASIO has no security related concerns about the prescribed administrative action. The legal definition of a *prescribed administrative action* is included in Appendix 2.

Public concerns about ASIO reliance on certain sources of information

3.13 As discussed in Chapter 1, concerns have been raised about the potential for ASIO to rely on government information from an IMA's country of origin in making security assessments. In response to these concerns, ASIO's Director-General has stated:

> One issue that I would really like to put to bed in as unequivocal terms as I possibly can is the notion that ASIO somehow conducts its security checks and makes its assessments based on information provided by the government of the country from which that immigrant has come. I can give you a categorical assurance that ASIO's policy, in accordance with government policy and with Australia's international obligations, does not refer the names of individuals who have sought asylum in Australia to the host government. We just do not do it. So our decisions are not, therefore, made on the basis of information provided about an individual from the host government.[81]

3.14 In conducting this audit, the ANAO observed that ASIO used a variety of relevant sources of information while conducting security assessments. ASIO considers, among other factors, the weighting, timeliness and reliability of available sources of information used during the assessment process.

Conclusion

3.15 ASIO staff are well-trained and follow clearly defined procedures in conducting security assessments.[82] All 411 cases examined by the ANAO complied fully with ASIO's processes and procedures. In terms of the appropriateness of the judgements made by ASIO assessors[83], there are quality assurance processes in place for the small proportion of security assessments that result in prejudicial advice. However, for those assessments that result in non-prejudicial advice, the quality assurance processes are not as robust and vary across assessment categories. Given that a security assessment may contribute to a client agency's decision to allow a person entry to Australia or access to sensitive information and/or locations, it would be prudent for ASIO to have in place a consistent quality assurance process to periodically validate,

---

[81] Parliamentary Joint Committee on Intelligence and Security, Canberra, 16 June 2011, pp.15-16.

[82] The procedures followed by ASIO are classified. The ANAO based its analysis on the application of these procedures.

[83] The ANAO did not seek to 'second guess' the judgements arrived at by ASIO officers conducting particular security assessments.

on a sample basis, its non-prejudicial security assessments for all security assessment types.

Recommendation No.3

3.16 To provide greater assurance of the security assessment process in the visa security assessments stream, the ANAO recommends that ASIO institute periodic quality assurance checks (on a sample basis) for security assessments that have been issued with non-prejudicial advice.

ASIO response: *Agreed.*

The Security Triaging Framework

3.17 Prior to April 2011, it was government policy that all IMAs who arrived in Australia be subject to security assessments that involved a full investigative process. Under a 'parallel processing' arrangement, ASIO conducted security investigations of IMAs at the same time as DIAC was determining the IMA's claims to refugee status. At the time, all security assessments for IMAs were treated by ASIO as complex investigations. The approach proved difficult to sustain when the numbers of IMAs increased. ASIO has described parallel processing as 'wasting a lot of effort'.[84]

3.18 In late 2010, the Government made two significant decisions to streamline the security assessment process and reduce the number of IMAs being referred to ASIO for security assessment. The first was that only those IMAs found to be refugees, and therefore eligible to apply for a visa, would be referred to ASIO for visa security assessments.

3.19 The second decision was to apply an intelligence-led and risk-managed approach to enable ASIO to focus on investigating security threats posed by people in the IMA stream. In practice, this meant that ASIO would be able to focus resources on the more complex cases. This process is known as the Security Triaging Framework (STF).

3.20 The STF involves an ASIO triaging team initially processing IMA referrals from DIAC. These IMAs have been confirmed as meeting the definition of a 'refugee' and may therefore require security assessments. On receiving the referrals, the triaging team conducts initial security checks based

[84] Official Committee Hansard, Legal and Constitutional Affairs Legislation Committee Estimates, 25 May 2011, p.107.

on ASIO's security indicators. The triaging team then makes a decision as to whether the IMA will be referred for further investigation within the BISA branch for a more thorough security assessment, or sent back to DIAC for protection visa processing.

3.21 Following ASIO developing the STF proposal in August 2010, an agreed joint position was negotiated with DIAC and agreed by the National Security Committee in December 2010. ASIO provided DIAC with details of the full framework in January 2011, and held the expectation of early implementation. However, DIAC did not implement the STF until April 2011. The impetus for introducing the STF at this time was the Christmas Island detention centre riots the previous month.

3.22 To date, government and DIAC's responses to the STF have been very positive. Both ASIO and DIAC advised that the backlogs within both agencies have been reduced, and the STF is considered to be a more efficient way of processing IMA assessments. Although the STF has proved to be an effective response to the changing caseload, it took an extended time to negotiate and implement. During this time ASIO's IMA security assessment backlog nearly doubled from 1500 to almost 3000 pending cases (Chapter 4 discusses caseload issues, including backlogs in more detail).

3.23 While the STF has been effective in reducing security assessment and related visa backlogs within both agencies, the ANAO identified administrative weaknesses in the triaging process. There are no documented standard operating procedures for the STF, and the team is heavily reliant on the team leader's expertise. Further, the IT tools used by the triaging team are very basic and potentially unstable. The triaging team uses Excel spreadsheets received from DIAC, which are manually 'cleaned', copied and pasted to produce various reports prior to triaging. There is a clear risk of losing important data and introducing, or retaining, errors in such a manual process.

Conclusion

3.24 The STF was introduced to streamline the security assessment process and reduce the number of IMAs being referred to ASIO for security assessment. Although the STF took an extended time to negotiate and implement, both ASIO and DIAC advised that the backlogs within both agencies have been reduced, and the STF is considered to be a more efficient way of processing IMA assessments. However, there are no documented standard operating procedures for the STF, and the team is heavily reliant on the team leader's expertise. The IT tools used by the triaging team are very

basic and potentially unstable, and there is a clear risk of losing important data and introducing, or retaining, errors through the manual processes being adopted. Consideration should be given, on a cost-benefit basis, to enhancing the supporting IT tools for the STF initiative.

Recommendation No.4

3.25 To better sustain the Security Triaging Framework initiative, the ANAO recommends that ASIO documents standard operating procedures for staff, and works with DIAC to enhance the supporting IT tools for the initiative.

ASIO response: *Agreed.* ASIO notes that documented standard operating procedures exist for staff undertaking triaging in relation to IMA cases.[85]

Responding to an emerging area of risk: security checks for community detention cases

3.26 Community-based detention arrangements were introduced in June 2005 to enable non-citizens who do not hold a visa to reside in the community without needing to be escorted. Community-based detention arrangements do not give a person any lawful status in Australia, nor does it give them the rights and entitlements of a person holding a visa living in the community (for example, the right to study or work). The person remains, administratively, detained under migration law while living in the community. Conditions include a mandatory requirement to report regularly to DIAC and/or their service provider,[86] and reside at the address specified by the Minister for Immigration and Citizenship.[87]

3.27 Only the Minister for Immigration and Citizenship can approve the necessary 'residence determination' to enable people in restrictive immigration detention to be released into community detention. The minister must consider what is in the public's best interest when making, varying or revoking a

[85] DIAC has indicated that it supports this recommendation and welcomes the opportunity to work with ASIO to enhance the Security Triaging Framework initiative.

[86] The lead service provider for this program is Red Cross. Services are also provided by Hotham Mission Asylum Seeker Project, Mercy Community Services, The Salvation Army, Multicultural Development Association, MacKillop Family Services and Marist Youth Care. These service providers are supported by subcontracted non-government organisations in providing care to clients. Red Cross is also the lead provider of services for unaccompanied minors in partnership with a range of specialist services providers.

[87] Department of Immigration and Citizenship, Fact Sheet 83a – Community Detention.

residence determination under the *Migration Act 1958*. This is a non-compellable power.[88]

3.28 In October 2010, the Minister for Immigration and Citizenship announced the expansion of an existing community detention program to children and vulnerable family groups. He stated that individuals will only be granted 'residence determination' if they are not considered a risk to the community and are assessed as unlikely to flee.

3.29 DIAC and ASIO agreed to implement a streamlined security check for certain adult IMAs identified for residence determination who had not yet received a full security assessment in relation to a grant of a visa. At the time of the announcement, it was expected that around 900 IMAs would be moved into community detention between October/November 2010 and June 2011. Of these 900, ASIO expected at the time to be referred around 200 cases for streamlined security checks, based on ASIO's understanding that these individuals were low-risk (adults in a cohort comprising vulnerable family groups and unaccompanied minors).

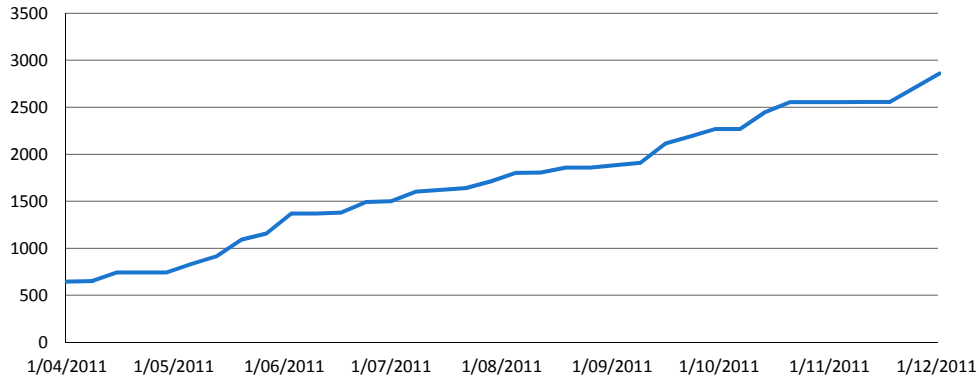
Substantial increase in the number of security checks

3.30 In 2011, the number of security checks for the purposes of community detention increased substantially. Figure 3.2 below illustrates the increase in the number of referred and assessed cases for community detention from 1 April to 2 December 2011.

[88] ibid.

Figure 3.2

Referred and assessed cases for community detention from April to December 2011



Source: ANAO analysis.

3.31 In eight months (as illustrated in Figure 3.2 above), the monthly number of security checks increased by almost 500 per cent, from 644 cases in April 2011 to 2858 cases in December 2011. The trend is likely to continue as DIAC has requested that all IMAs be referred to ASIO for community detention security assessments rather than the initial smaller cohort of low-risk cases. Responding to the security assessment consequences of the large increase in the number of IMAs being assessed for potential release into community detention (from small numbers to hundreds per week)[89]; and the increase in the type of cohorts that will be put into community detention (from the vulnerable IMAs to all IMAs) has proved to be a challenging task for ASIO. Initially, ASIO applied specific security indicator thresholds to its community detention assessments that were consistent with the overall low-risk nature of the expected caseload.

3.32 In November 2011, ASIO appropriately revised its security assessment thresholds for community detention in light of the changing risk profile of the community detention cohort. The same threshold now applies across all IMA security assessments. ASIO will therefore issue an adverse security assessment in relation to community detention if the IMA was assessed as representing a direct or indirect risk to security.

[89] ASIO advised that, as at the time of the audit, only a small proportion of those IMAs 'cleared' for community detention had actually been transferred.

3.33 ASIO also advised that there have been between five and 10 cases where IMAs have been referred to ASIO for community detention security assessments despite ASIO having already issued an adverse security assessment or qualified security assessment in relation to a grant of a visa. As discussed previously, such persons are not eligible for release into community detention.

Reporting risks posed by growth in community detention

3.34 Decisions on detention policies are matters for Government, taking into account advice from key policy agencies, such as DIAC, and specialist agencies, such as ASIO. In this regard, aspects of the security risks posed by the changing nature of community detention arrangements have been identified by ASIO as concerning and have been raised internally and with key agency stakeholders and the Government. In November 2011, the IGIS announced an inquiry into the handling by ASIO of referrals made by DIAC for community detention security assessments for individuals in immigration detention.

Conclusion

3.35 In October 2010, the Minister for Immigration and Citizenship announced the expansion of an existing 'residence determination' program (community detention) to children and vulnerable family groups. DIAC and ASIO agreed to implement a streamlined security check for certain IMAs identified for residence determination but who had not yet received a full security assessment in relation to a grant of a visa. At the time of the announcement, it was expected that around 900 IMAs would be moved into community detention between October/November 2010 and June 2011. Of these 900, ASIO expected at the time to be referred around 200 cases for streamlined security checks. In 2011, the number of security checks for the purposes of community detention increased substantially. In eight months, the monthly number of security checks increased by almost 500 per cent, from 644 cases in April 2011 to 2858 cases in December 2011. The trend is likely to continue as DIAC has requested that all IMAs be referred to ASIO for community detention security assessments rather than the initial smaller cohort of low-risk cases.

3.36 Responding to the security assessment consequences of the large increase in the number of IMAs being assessed for potential release into community detention has proved to be a challenging task for ASIO. Aspects of the security risks posed by the changing nature of community detention

arrangements have been identified by ASIO as concerning and have been raised internally and with key agency stakeholders and the Government.

4. Workload and Performance Trends for Security Assessments

This chapter examines workload and performance trends in ASIO's security assessments.

Introduction

4.1 As previously discussed, a changing security environment, the increase in IMAs and the then policy to refer all IMAs to ASIO for security assessments, placed pressure on ASIO's capacity to provide timely security assessments. In this context, the ANAO examined workload and performance trends in ASIO's security assessments in terms of:

- referrals received and pending cases; and
- processing times.

Referrals received and pending cases

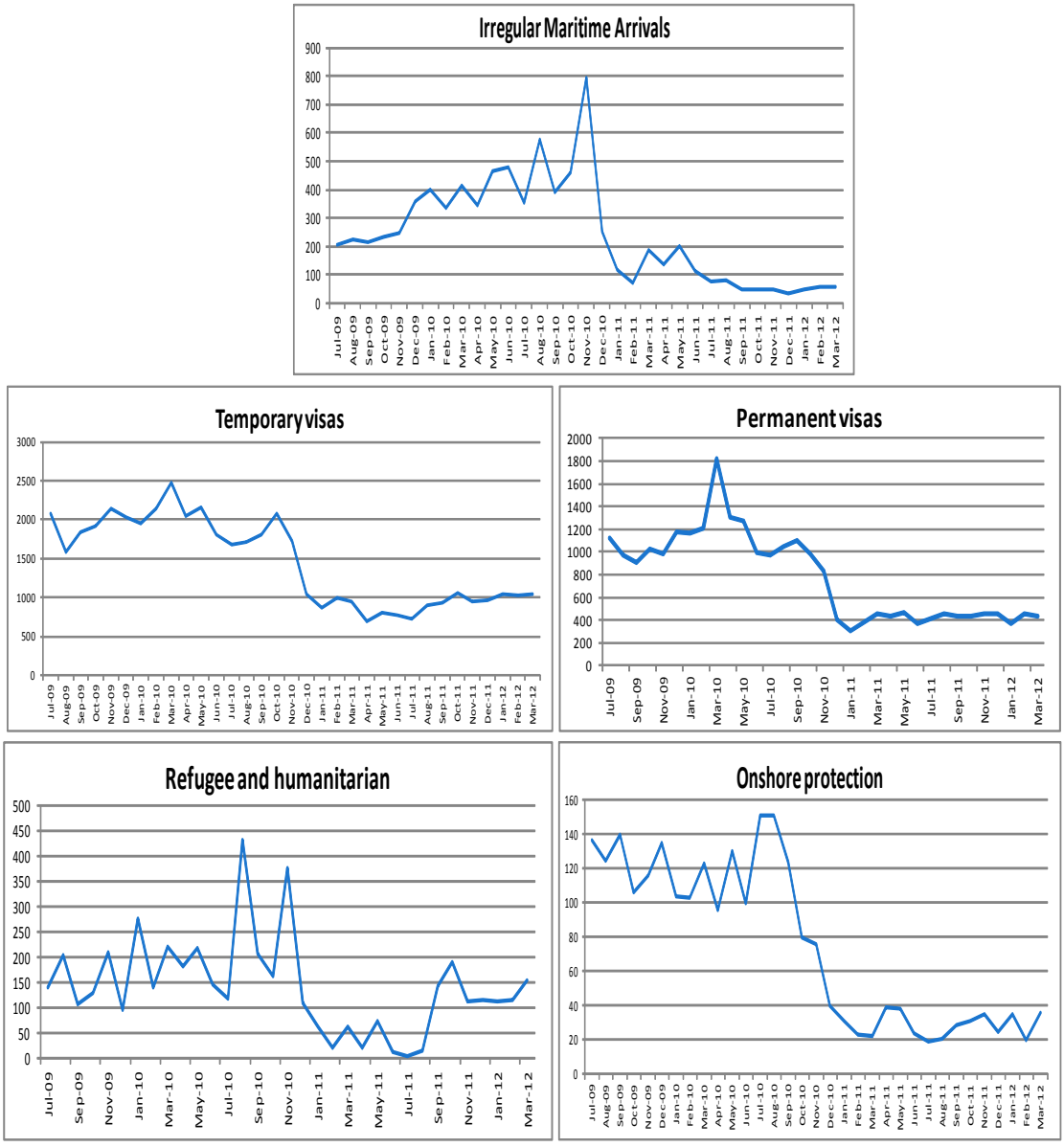
4.2 As discussed in Chapter 1, the completion rate of ASIO's security assessments have fluctuated over the years, with no discernable trend. In its public reporting, ASIO has only ever reported on the number of assessments completed across the main security assessment categories: visa security assessments stream; personnel security assessments and counter-terrorism security assessments. Such output measures do not give a complete picture of trends in the assessment caseload. In the following sections, the ANAO outlines workload trends in terms of: referrals received and the pending cases.

Referrals received

4.3 Figure 4.1 and Figure 4.2 below illustrate the referrals received by ASIO across all the security assessment categories for the period 2009–10 to 2011–12 (up to March 2012).

Figure 4.1

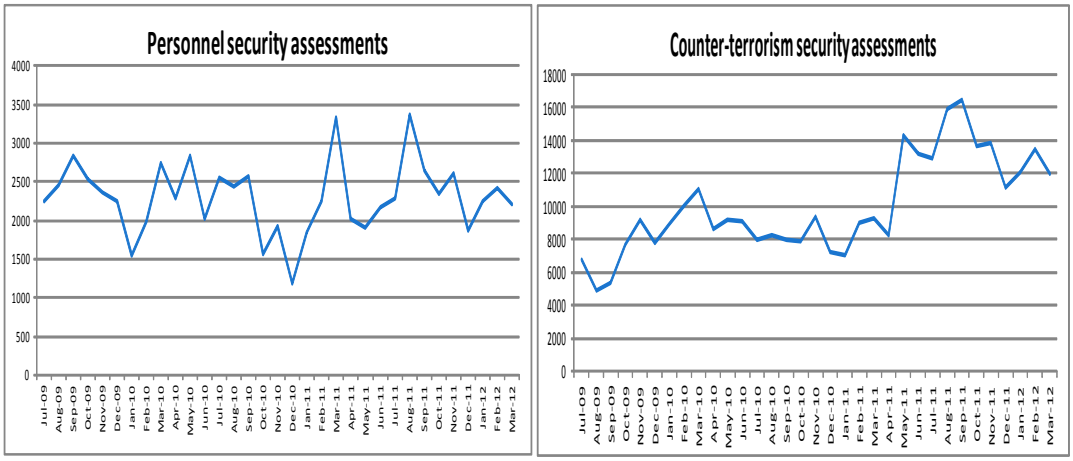
Number of referrals received across the visa security assessments stream July 2009 to March 2012



Source: ANAO analysis of ASIO data.

Figure 4.2

Number of referrals received across personnel and counter-terrorism security assessment categories July 2009 to March 2012



Source: ANAO analysis of ASIO data.

4.4 The number of referrals received by ASIO across all security assessment categories has fluctuated over time. Referrals received for IMAs increased steadily from 2009 and peaked in the last quarter of 2010, reflecting the number of people arriving by 'suspected illegal entry vessels' and the Government's then policy of referring all IMAs to ASIO for security assessments. The substantial decline of referrals in the first half of 2011 reflects the new intelligence-led, risk management approach (the security triaging framework) as discussed in Chapter 3. Referrals for both temporary and permanent visas peaked at various points in 2009–10. Referrals for refugee/humanitarian cases and onshore protection cases peaked in the second half of 2010, and declined substantially in the first half of 2011.

4.5 Similarly, referrals for both personnel security assessments and counter-terrorism security assessments fluctuated from July 2009 to March 2012.

Pending cases

Pending cases resulting to backlogs

4.6 Pending cases are client agency referrals that have been received by ASIO and are in the queue to be security assessed or for final security

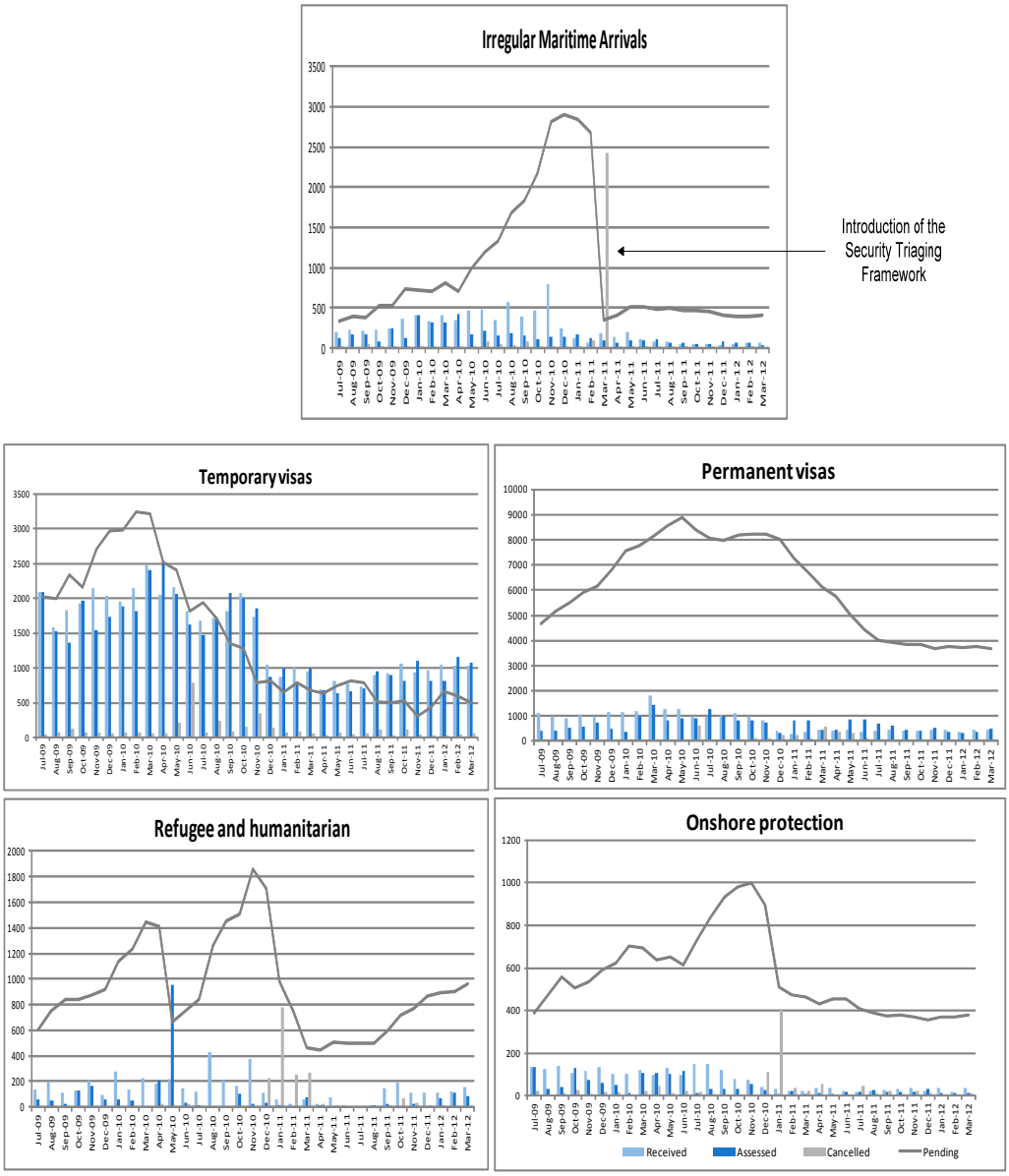
assessment.[90] Having a modest level of pending cases is important in managing workflow in a client service environment. However, an accumulation of unfinished security assessments will result in an undesirable backlog. With the increase in IMAs stretching the processing capacity of ASIO, turnaround times for processing security assessments exceeded expected timeframes across all security assessment categories. Backlogs ensued as the demand for security assessments exceeded the output capacity of ASIO staff.

4.7 Pending cases across these visa security assessment categories for the period 2009–10 and 2010–11 are illustrated in Figure 4.3 below.

[90] Cases in the pending caseload may be undergoing active investigation, but not finalised.

Figure 4.3

Pending cases across the visa security assessments stream July 2009 to March 2012



Source: ANAO analysis of ASIO data.

4.8 The pending cases trend across the visa security assessment categories followed a consistent pattern, albeit with differing numbers of cases. In each category, the number of pending cases grew rapidly over a period of months,

and then fell as the backlog was brought under control. The ANAO noted the following:

- **Irregular maritime arrivals**—the pending caseload peaked in December 2010 at 2908 cases. The caseload declined dramatically in the first quarter of 2011, from 2679 pending cases in February 2011 to 345 cases in March 2011, and increasing slightly to 511 pending cases in June 2011. This reflects the implementation of the security triaging framework, as discussed in Chapter 3. The average number of cases assessed from 2009–10 and 2010–11 was 178 per month.
- **Temporary visas**—the pending caseload peaked in late 2009 and early 2010. The biggest backlog was in February 2010 with 3245 cases on hand. The number of pending cases started to decline in the last quarter of 2010 through the first half of 2011, with 820 pending cases reported in June 2011. The average number of cases assessed from 2009–10 to 2010–11 was 1555 per month.
- **Visas for permanent residence**—the pending caseload for this stream was the largest when compared to other visa security assessment categories. The peak backlog was experienced in May 2010 with 8902 cases on hand. The number of pending cases had been consistently high from the second-half of 2009 to the first quarter of 2011. The number of pending cases in June 2011 was 4421, closer to the figure reported two years prior (in July 2009) of 4654 cases. From 2009 to 2011, there were large disparities between the number of cases assessed and the number of cases pending. The average number of cases assessed for this period was 745 per month.
- **Offshore refugee/humanitarian**—the pending caseload peaked in the second-half of the 2010 reporting period, with the biggest backlog in November 2010, of 1859 pending cases.[91] The backlog improved in the first-half of 2011, with 499 pending cases reported as at June 2011. The average number of cases assessed for the 2010–11 reporting period was 27 cases per month.
- **Onshore protection**—the pending caseload increased in the second-half of 2010, with the biggest backlog in November 2010 of

[91] The caseload was temporarily suspended in the first quarter of 2010–11 pending the outcome of a team established to review and prioritise the caseload.

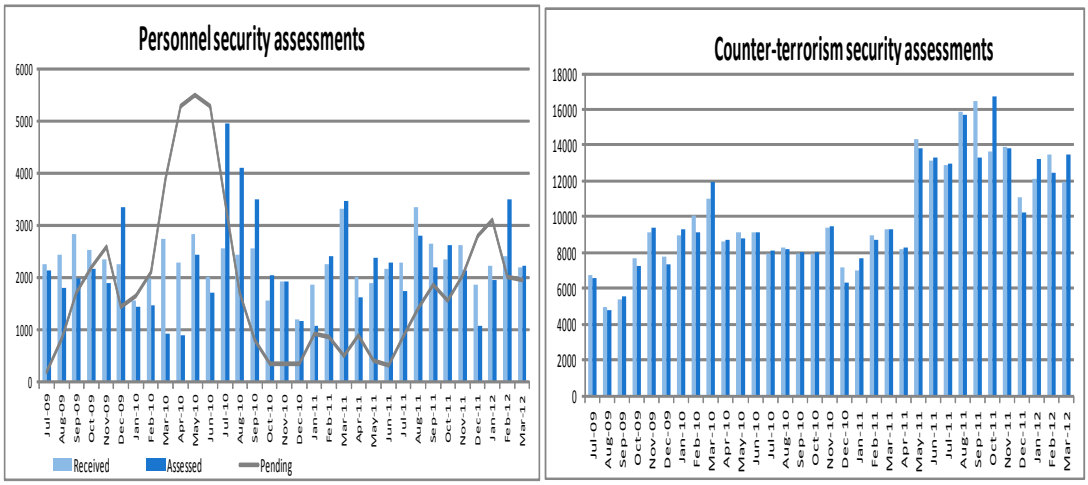
999 cases on hand. The backlog started to abate in 2011 with 457 cases pending as at June 2011. The average number of cases assessed for 2010–11 reporting period was 24 cases per month.

Pending cases across personnel and counter–terrorism security assessment categories

4.9 Pending cases across the personnel and counter-terrorism security assessment categories are illustrated in Figure 4.4 below.

Figure 4.4

Pending cases across personnel and counter–terrorism security assessment categories July 2009 to March 2012



Source: ANAO analysis of ASIO data.

4.10 The ANAO noted the following pending cases trend across the personnel and counter-terrorism security assessment categories:

- **Personnel security assessments**—the pending caseload for this stream peaked in April to June 2010, with a high of 5500 cases recorded in May 2010. It started to decline in September 2010 with 820 pending cases, improving further to 370 pending cases in December 2010. In July 2011, there were 860 pending cases and by January 2012, there were 3100 pending cases recorded. The average number of cases assessed from July 2009 to March 2012 was 2237 per month.
- **Counter-terrorism security assessments**—there are no pending cases shown in this stream as illustrated in Figure 4.4. Counter-terrorism security assessments are always given priority compared to personnel

security assessments, and therefore the pending cases, if any, are negligible.

4.11 The ANAO observed that the pending caseload is closely monitored by the relevant line areas within ASIO. In addition, as discussed in Chapter 2, the relevant security assessment branches have addressed issues and risks relating to pending cases and resulting backlogs in their Quarterly Performance Reports to the ASIO Executive and in their risk treatments plans.

Processing times

4.12 The aspect of ASIO's security assessment process that has attracted the most public comment and criticism in recent years is its timeliness. The following sections outline: the time standards that have been set for the processing of security assessments; ASIO's performance against these standards; and the ANAO's observations about the key factors that affected assessment timeframes.

Time standards

4.13 Given the importance of ASIO security assessments to the finalisation of client agency processes, it would be reasonable to expect that ASIO and its client agencies would have settled on time standards for the provision of security assessments. The ANAO found that, in relation to visa security assessments, no time standards have been formally settled between ASIO and DIAC, although an informal agreement has been reached on some visa security assessment types. These standards (outlined in Table 4.1) are, in the main, consistent with those published by DIAC in relation to expected visa processing times.[92]

4.14 For IMAs whose identities and intentions can be difficult to verify and assess, there is no formal or informally agreed time standard. The complexity of such cases militates against the practicality of setting time standards. In ordinary circumstances, when factors such as the identity and status of the visa applicant that affect the processing of security assessments are known, it is easier to set and agree on a time standard. However, in extraordinary cases where an applicant is unknown, refuses to divulge details about himself/herself, or conceals his/her identity, it becomes complex and difficult to set and agree on time standards to process the security assessment.

[92] See: <www.immi.gov.au/about/charters/client-services-charter/visas> [Accessed 30 April 2012].

4.15 There are also no time standards, formal or informal, settled between ASIO and AGSVA, for personnel security assessments. However, for counter-terrorism security assessments, time standards have been formally settled between ASIO and AusCheck in their Memorandum of Understanding.

4.16 Table 4.1 provides a summary of (formal and informal) agreed timeframes between ASIO and its client agencies. In relation to visa security assessments, ASIO requested that the informal time or service standards for specific visa classes not be included in this report.

Table 4.1

Time or service standards for various security assessment categories

Security assessment category	Client agency	ANAO comment
IMAs	DIAC	**No formal or informal agreed timeframes with DIAC.** All IMA security assessments are complex.
Various visas	DIAC	**Informally agreed with DIAC**. The informal standards set for security assessments for visa applicants range from one to six months, depending on the visa class.
Personnel	AGSVA and AGSVA exempt agencies.[93]	**No formal or informal agreed timeframes with AGSVA and AGSVA exempt agencies.** There is no formal agreement between AGSVA and ASIO on agreed timeframes. At the time of audit, AGSVA's service standards for the indicated clearance levels had not been discussed nor agreed with ASIO.
Counter-terrorism (CT)	AusCheck and AFP[94]	**There are formal agreed timeframes with AusCheck.** A signed MoU exists between ASIO and AusCheck that outlines the indicated service standard and timeframes, including ones for complex cases,[95] as follows: • 95 per cent within five business days; and • 75 per cent of remaining CT checks to be completed within 60 business days. There are no time or service standards for complex cases as they become ASIO investigations.

Source: ANAO analysis.

[93] The audit did not include AGSVA exempt agencies.

[94] CT security assessments for the AFP were not included in this audit.

[95] Although ASIO's MoU is with AusCheck, ASIO extends the conditions of the MoU for all CT security assessments, including those referred by the AFP.

Performance against the specified time standards

4.17 The ANAO assessed the timeliness of ASIO's assessments using its sample of 411 cases from ASIO's security assessment categories covering 2009–10 and 2010–11. The processing time for security assessments is the time taken from ASIO's receipt of the referral to the time a security assessment/advice is made/given to the client agency. A comparison was made between the service standards (formal/informal) and the processing times for the sampled cases[96]:

- **Irregular maritime arrivals**—66 cases examined. There are no time standards. The number of processing days for IMAs ranged between one day and 714 days (as shown in Table 4.2 below).
- **Temporary visas**—71 cases examined. Of these, 42 per cent were processed outside the informal standard.
- **Permanent visas**—68 cases examined. Of these, 35 per cent were processed outside the informal standard.
- **Onshore protection/refugee and humanitarian**—65 cases examined. Of these, 49 per cent were processed outside the informal standard. Of the 65 cases sampled, 24 were Protection Visa cases, and of the 24, 71 per cent were processed outside the informal standard.
- **Personnel**—72 cases examined. There are no time standards. The number of processing days for personnel cases ranged between completion on the same day to 679 days (as shown in Table 4.2 below).
- **Counter-terrorism**—69 cases examined. Of these, 90 per cent were processed within five days.

4.18 Overall, for all the security assessment categories, 34 per cent of cases in the sample exceeded the formal or informal expected timeframes. Informal processing times agreed with DIAC have been exceeded in many cases. While ASIO has formally set time or service standards with AusCheck, none have been formally set with DIAC and AGSVA. The absence of a formal agreement limits accountability between ASIO and its client agencies in such cases. Should formal arrangements with DIAC and AGSVA be established as recommended by the ANAO (Recommendation 2 at paragraph 2.54), there

[96] ASIO requested that the informal time or service standards for each visa class not be individually specified in this report.

would be merit in ASIO settling on reasonable processing times for non-complex cases with its key client agencies and agreeing arrangements to provide regular updates on the status of complex cases.

The time taken to process cases

4.19 The time taken to process security assessments varies within each category. Table 4.2. illustrates the average, and also the range of processing times for each category in the ANAO's sample.

Table 4.2

Shortest and longest number of processing days, and the mean processing days for each security assessment category

Security assessment category	Mean/average processing days	Shortest number of processing days	Longest number of processing days
IMAs	285	1	714
Temporary visas	37	0	360
Permanent visas	207	4	918
Onshore and offshore refugee/humanitarian	238	48	912
Personnel	20	Same day	679
Counter–terrorism	12	Same day	313

Source: ANAO analysis of audit sample.

4.20 As shown in Table 4.2, the average number of days to process IMAs, onshore and offshore refugee/humanitarian and permanent visa security assessments ranged from 207 to 285 days for the period, reflecting the complexities of the cases handled and DIAC and Government priorities. The average number of days to process temporary visas, personnel security and counter-terrorism security assessments ranged from 12 days to 37 days.

4.21 Security assessments for some non-complex cases can be conducted in less than a day, as shown in the categories for temporary visas, personnel and counter–terrorism. On the other hand, the ANAO sample shows that complex cases can have lengthy processing times, up to 918 days in one case.

Key factors that affect security assessment timeframes

4.22 A number of factors can affect the length of time it takes to process security assessments. Some key factors include: quality of information/data received from referring agencies; the increase in the number and complexity of

cases; changes in Government policies and client agencies' priorities (such as suspending processing of certain groups and prioritising the processing of others); staffing levels and backlogs. These factors are discussed in below.

Poor data quality or missing mandatory information

4.23 ASIO relies on the accuracy and completeness of information sent by its key client agencies, DIAC and AGSVA. At the time of audit, ASIO has been receiving referrals containing poor quality data or missing mandatory information which has contributed to delays in processing security assessments.

Changes in the volume and complexity of the assessment caseload

4.24 The complexity of the security assessment caseload has changed over the past decade, driven in particular by the sharp increase in IMAs in recent years (as discussed in Chapter 1). This increase in the volume of IMAs has had a significant impact on security assessment processing. The population of IMAs in detention has increased from approximately 1563 at the end of January 2010 to 7147 IMAs in December 2011, an increase of almost 500 per cent (as shown in Table 1.2). The change in IMA movements has been variously attributed to push factors overseas, such as global movements and uncertainties, particularly adverse events such as civil strife, war, persecution, environmental disasters and poverty, and pull factors in Australia, such as the state of the Australian economy and migration policy settings. In 2010, IMA arrivals outpaced the number of security assessments ASIO could process resulting in the lengthy assessment times and backlogs.

Increased scrutiny of certain IMAs

4.25 With the increase in boat arrivals in 2009 and 2010, it became apparent to both ASIO and DIAC that some groups were proving to be more difficult to process than others. Some IMAs that passed through initial DIAC and ASIO checks were, upon more detailed ASIO investigation, being assessed as a security risk to Australia. Consequently, in April 2009, ASIO decided to increase the scrutiny of a higher-risk IMA group. As a consequence of this increased scrutiny, more time and effort was exerted to conduct security assessments for this particular group.

DIAC (and Government) decisions to prioritise the IMA caseload

Expedite release of detainees from Christmas Island IDC

4.26 Since July 2009, DIAC had been advising ASIO to prioritise IMA cases that were already onshore and detained in Immigration Detention Centres (IDCs). In January 2010, DIAC advised ASIO to prioritise processing of

non-complex cases in order that accommodation could be freed up at the Christmas Island IDC. The increase in boat arrivals was putting pressure on the capacity of IDCs. DIAC indicated that the Government's expectation at the time was to increase the speed by which IMAs were being processed. It also advised that it was willing to prioritise certain groups instead of working sequentially through each group of boat arrivals, as had been past practice.

4.27 DIAC's expectation was for ASIO to process 100 IMAs (or more) each week, and ensure that 10-15 of these were of a particular group. The agency gave ASIO a prepared list of names and dates of release. ASIO did not agree to the pre-determined list by a particular date, but agreed to review its organisational resources to ensure that ageing (complex) caseload continued to be finalised. A consequence of this approach was that ageing, complex cases were put aside by ASIO to free up resources to process non-complex cases.

Protection visas and refugee/humanitarian caseloads temporarily suspended

4.28 Also in January 2010, DIAC advised ASIO to temporarily suspend assessments for protection visas and the refugee/humanitarian cases as IMA cases were considered a higher priority for DIAC and the Government. There was pressure to increase the number of IMA security assessments, which was already consuming most of ASIO's resources in the security assessment line areas. Consequently, the 90-day informal processing standard was exceeded for the protection visa caseload, leading to the substantial backlogs in this security assessment category that was still evident in 2010 and 2011.

Government suspension of new asylum applications from Sri Lanka and Afghanistan

4.29 In April 2010, the Government suspended the processing of new asylum applications and claims from Sri Lankan nationals for a period of three months, and claims by Afghan nationals for a period of six months,[97] because of the evolving circumstances in these two countries.[98] Afghans and Sri Lankans were two of the top nationalities that were arriving by boat at that time. As a result, from mid-2010 to 2011, ASIO had large backlogs in the visa

[97] Minister for Immigration and Citizenship media announcement, *Changes to Australia's Immigration Processing System*, 9 April 2010. <www.minister.immi.gov.au/media/mediareleases/2010/cel10029.htm>[Accessed 23 December 2011].

[98] In 2010, Sri Lanka and Afghanistan were both seen as evolving. Sri Lanka was assessed as a country in transition after two decades of conflict, with hopes for improvement and stabilisation in conditions. Afghanistan was also evolving, including with respect to Afghan Hazaras. <www.minister.immi.gov.au/media/mediareleases/2010/cel10029.htm>[Accessed 23 December 2011].

security assessment categories whose cases comprised mostly of Afghan and Sri Lankan nationals.

Prioritisation of Oceanic Viking cases

4.30 In October 2009 a Customs and Border Protection vessel, the Oceanic Viking, picked up asylum seekers after they issued a distress call in the Indonesian search and rescue zone. The asylum seekers then refused to leave the vessel and a stand-off ensued. Following discussions between the asylum seekers, Australian and Indonesian officials and the UNHCR, the group left the vessel.[99]

4.31 While some of the asylum seekers were resettled in Australia and Canada, media reports in January 2010 indicated that DIAC was still continuing to search for another country to resettle the remaining asylum seekers.[100] In October 2010, DIAC requested that ASIO prioritise the Oceanic Viking asylum seekers who were now in Romania (in a UNHCR emergency transit centre). Experienced officers from ASIO's IMA directorate were sent to Romania to process this group. This event also contributed to IMA backlogs that were still evident in 2010 and 2011 as a relatively large, experienced group of IMA assessors and/or analysts were reassigned to work on this project.

4.32 Table 4.3 summarises the ANAO's observations about the combined impact of these key factors on each security assessment category in the ANAO's sample.

[99] See: *Message from Jim O'Callaghan, Minister-Counsellor Immigration, Australian Embassy, Jakarta, Indonesia to the 78 passengers on the Oceanic Viking, November 2009*. Document presented by Mr Rudd, 16 November 2009 < http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22publications%2Ftabledpapers%2F50530%22> [Accessed 10 May 2012]. See also: *Letter from Andrew Metcalfe, Secretary, Department of Immigration and Citizenship to the Minister for Immigration and Citizenship, Senator Chris Evans, 16 November 2009*. Document presented by Mr Rudd, 16 November 2009 <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22publications%2Ftabledpapers%2F50529%22> [Accessed 10 May 2012].

[100] ABC news 'Four Oceanic Viking Tamils refused visas'<www.abc.net.au/news/2010-01-12/four-oceanic-viking-tamils-refused-visas/1205604> [Accessed 22 December 2011].

Table 4.3

ANAO sample: factors affecting processing timeframes

Security assessment category	ANAO observations
IMA security assessments	• Complex cases required extensive investigations for certain groups to determine identification of individuals. Some IMAs were providing false and contradictory statements. • Increase in the number of cases to process was matched by a corresponding staff increase. • Directly affected by DIAC processing priorities and Government policy changes. • Backlogs due to policy changes/processing priorities and pre-triage where ASIO was assessing all IMAs. • Lengthy response time to requests for additional information and property forensic reports. • Logistical issues when interviewing IMAs. Issues with regards to organising an appropriate interpreter; availability of interview rooms and additional preparatory work prior to deployment of ASIO staff.
Temporary visa security assessments	• Incomplete mandatory information from DIAC. • Backlogs. • Complex cases. • Responses to ASIO requests for more information were slow in some cases. For example, a case had been open for 231 days. It went back to the DIAC post for more information, and at the time of audit, it was still ongoing. • Indirectly affected by Government policy changes and DIAC processing priorities.
Permanent visa security assessments	• Incomplete mandatory information from DIAC. • Backlogs, due to internal staff movements or staff leaving. • Number of complex cases increased, applicants that trigger ASIO's security indicators took a longer time to process. • A number of cases were with DIAC for a period of time before being referred, or re-referred, to ASIO. For example, a case was with DIAC since 2005, and was referred to ASIO in 2008. A request for more information by ASIO required three follow-ups. • Indirectly affected by Government policy changes and DIAC processing priorities.
Onshore protection and Offshore refugee/humanitarian visa security assessments	• Directly affected by Government policy changes and DIAC processing priorities, particularly when ASIO was directed to cease work on specific groups. • Certain policy changes affected timeframes. • In 2009–10, there was no dedicated staff to process these cases.

Security assessment category	ANAO observations
Personnel security assessments	• Counter-terrorism security assessments are given priority over personnel security assessments. • Numerous instances of poor data or incomplete mandatory information from referring agencies which required separate email communications to resolve. • Complex cases often required detailed and complex ASIO investigations, often in cooperation with other ASIO subject areas and other domestic and international partners. Security questionnaires and lengthy interviews often required. • Backlogs due to staff movements and resourcing.
Counter-terrorism security assessments	• Incomplete information from sponsoring agency. • Complex cases often required detailed and complex ASIO investigations, often in cooperation with other ASIO subject areas and other domestic and international partners. Security questionnaires and lengthy interviews often required. • Applicants not turning up for the ASIO interview.

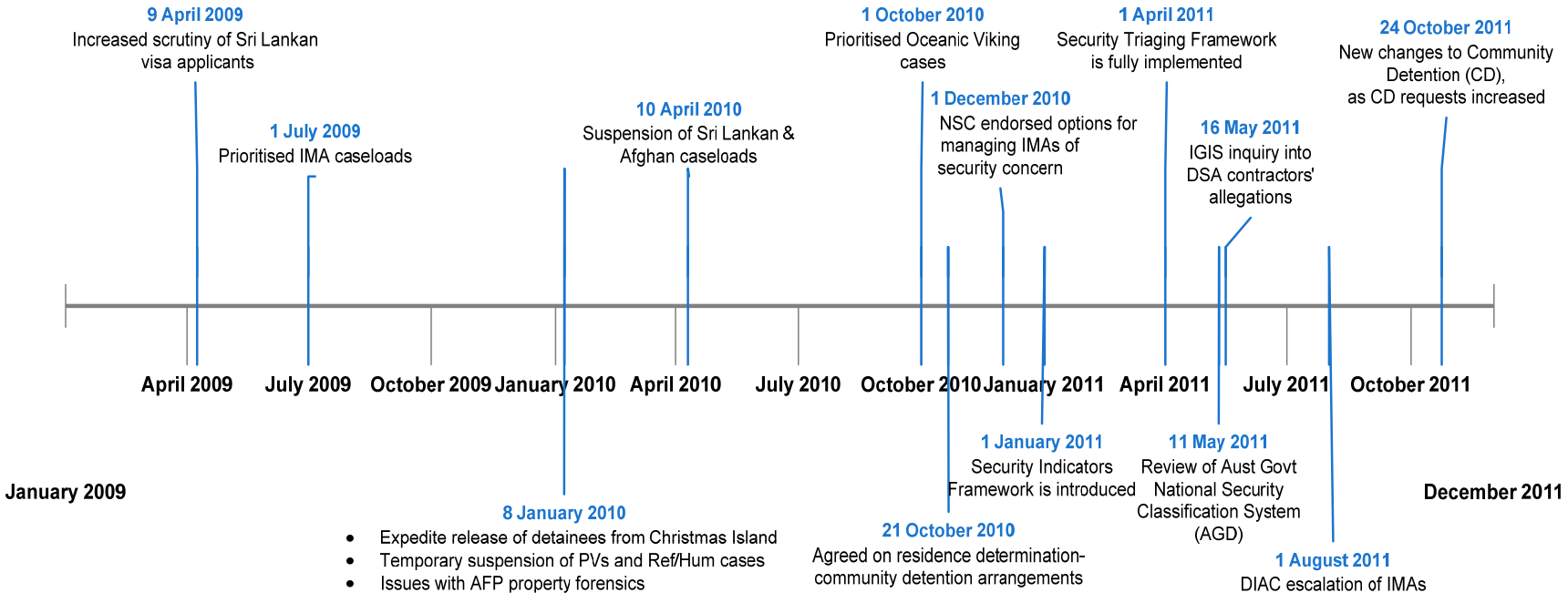
Source: ANAO analysis of ASIO data.

4.33 Overall, the processing of each security assessment category has been affected differently by the various issues observed by the ANAO. However, ASIO management particularly highlighted the combined operational impact of the changes in Government policies and agency processing priorities in the visa security assessment stream.

4.34 Figure 4.5 illustrates the timeline of key events and decisions that affected ASIO's timeframes for security assessment processing in 2009–2011.

Figure 4.5

Timeline of key events and decisions that affected ASIO's timeframes security assessment processing (2009–11)



Source: ANAO analysis of ASIO data.

The priority given to national security considerations in completing investigations for security assessments

4.35 A number of initiatives have been put in place to expedite the security assessments process, such as the introduction of the STF (as discussed in Chapter 3). The Government[101] and ASIO have highlighted that 'Australia's national security considerations take precedence at all stages'.[102]

4.36 The ANAO observed that across the relevant security assessment categories, ASIO assessors and analysts are mindful of the (formal or informally agreed) time standards that have been set either by ASIO or its key client agencies, and endeavour to meet these standards. However, when cases become complex and require further investigation, analysis, or reliance on sources of information that may be external to the agency—the security assessment process will take longer than expected. As in any intelligence investigation, the collection and analysis of information takes time, and will vary from case to case.

4.37 ASIO's approach is to continue its investigation and analysis of a case until such time as its assessors or analysts are satisfied that the information they have of an individual is sufficient and appropriate to warrant a non-prejudicial, adverse or qualified assessment.[103]

Conclusion

4.38 A variety of factors have contributed to the time taken to process security assessments, some of which are beyond ASIO's direct control. These factors include the increase in the number and complexity of cases, and changes in Government policies and client agencies' priorities.

4.39 Backlogs occurred when the demand for security assessments exceeded the output capacity of ASIO staff. Processing times have only been formally agreed with one client agency, AusCheck. No time standards have been

[101] On 4 December 2008, the then Prime Minister Kevin Rudd presented the first National Security Statement to the Australian Parliament. It stated that 'the first priority of government is the nation's security.'

[102] ASIO Report to Parliament 2010-11, p. 24.

[103] There are instances when ASIO will cease a security assessment investigation, these occur when: an applicant withdraws their application for a visa, or DIAC would cancel a referral for a security assessment as the visa application has been rejected on other grounds. Despite ceasing a security assessment, the profile or case details of an individual for whom a security assessment has commenced will remain in ASIO's systems.

formally agreed between ASIO and DIAC, or by ASIO and AGSVA, for any security assessments. However, informal agreements had been reached with DIAC on some visa security assessments.

4.40 ANAO analysis showed an increasing trend in the number of pending cases or backlogs across all security assessment categories in 2009–10 and 2010–11, with prolonged processing times for some categories. Thirty four per cent of cases sampled across all the security assessment categories exceeded the expected timeframes, or have prolonged processing times. Conversely, ANAO analysis of personnel and counter-terrorism security assessments showed that 75 per cent and 90 per cent of cases were processed within a day (for personnel) and five days (for counter-terrorism), respectively.

Ian McPhee
Auditor-General

Canberra ACT
25 June 2012

Appendices

Appendix 1: Agency Response

Australian Government

Australian Security Intelligence Organisation

Director-General of Security

28 May 2012
eA1230997

Mr Ian McPhee PSM
Auditor-General
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Ian,

ASIO response to ANAO audit of security assessments

Thank you for the opportunity to comment on the proposed report from the Australian National Audit Office on *Security Assessments of Individuals*.

ASIO welcomes the findings of the audit report, in particular the assessment that ASIO's arrangements for providing security assessments of individuals are robust and effective. We have provided comments below in relation to the recommendations in the report, which we hope you will find useful in the preparation of the final report.

Recommendation	Response
Recommendation 1 To strengthen workforce planning strategies, including for a contingency or surge capacity for the security assessment branches, the ANAO recommends that ASIO: • periodically re-assesses staffing levels of the security assessment branches based on current and projected risks, priorities, and caseloads; and • develops a workforce plan for the Security Assessments and Border Investigations Division.	Agree. ASIO regularly assesses staffing levels across the Organisation in the context of its Strategic Risk Management Framework and intelligence priorities.

GPO Box 2176
Canberra City ACT 2601
Telephone: 02 6249 6299
Facsimile: 02 6257 4501

Recommendation 2 To strengthen working relationships, service delivery arrangements and the sharing of information with client agencies, the ANAO recommends that ASIO establishes formal arrangements with key client agencies that address operational matters including: • ongoing liaison and problem resolution arrangements; • reasonable processing times for non-complex cases; • arrangements to provide regular updates on the status of complex cases; and • data quality expectations.	Agree. ASIO will continue to progress MoUs with client agencies. In relation to regular updates on complex cases, ASIO will continue to liaise with client agencies as required on complex cases. The nature of investigative work and its reliance on external exigencies means timeframes for investigations must necessarily be indicative only.
Recommendation 3 To provide greater assurance of the security assessment process in the visa security assessments stream, the ANAO recommends that ASIO institute periodic quality assurance checks (on a sample basis) for security assessments that have been issued with non-prejudicial advice.	Agree.
Recommendation 4 To better sustain the Security Triaging Framework initiative, the ANAO recommends that ASIO documents standard operating procedures for staff, and works with DIAC to enhance the supporting IT tools for the initiative.	Agree. ASIO notes that documented standard operating procedures exist for staff undertaking triaging in relation to IMA cases.

ASIO has welcomed the opportunity to contribute to the performance audit, *Security Assessments of Individuals*, and thanks those ANAO staff involved for their professional engagement during the audit process.

Yours,

David Irvine

David Irvine

Appendix 2: Definition of a prescribed administrative action

Part IV Section 35 of the ASIO Act defines a prescribed administrative action as:

(a) an action that relates to or affects:

> (i) access by a person to any information or place access to which is controlled or limited on security grounds; or
>
> (ii) a person's ability to perform an activity in relation to, or involving, a thing (other than information or a place), if that ability is controlled or limited on security grounds; including action affecting the occupancy of any office or position under the Commonwealth or an authority of the Commonwealth or under a State or an authority of a State, or in the service of a Commonwealth contractor, the occupant of which has or may have any such access or ability;

(b) the exercise of any power, or the performance of any function, in relation to a person under the *Migration Act 1958* or the regulations under that Act; or

(c) the exercise of any power, or the performance of any function, in relation to a person under the *Australian Citizenship Act 2007*, the *Australian Passports Act 2005* or the regulations under either of those Acts; or

(d) the exercise of a power under section 58A, or subsection 581(3), of the *Telecommunications Act 1997*.

Note: An obligation, prohibition or restriction imposed by a control order is not prescribed administrative action.

Index

S

T

U

V

W

Series Titles

ANAO Audit Report No.1 2011–12
The Australian Defence Force's Mechanisms for Learning from Operational Activities
Department of Defence

ANAO Audit Report No.2 2011–12
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2010 Compliance)

ANAO Audit Report No.3 2011–12
Therapeutic Goods Regulation: Complementary Medicines
Department of Health and Ageing

ANAO Audit Report No.4 2011–12
Indigenous Employment in Government Service Delivery

ANAO Audit Report No.5 2011–12
Development and Implementation of Key Performance Indicators to Support the Outcomes and Programs Framework

ANAO Audit Report No.6 2011–12
Fair Work Education and Information Program
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.7 2011–12
Establishment, Implementation and Administration of the Infrastructure Employment Projects Stream of the Jobs Fund
Department of Infrastructure and Transport

ANAO Audit Report No.8 2011–12
The National Blood Authority's Management of the National Blood Supply
National Blood Authority

ANAO Audit Report No.9 2011–12
Indigenous Secondary Student Accommodation Initiatives
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.10 2011–12
Administration of the National Partnership on Early Childhood Education
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.11 2011–12
Implementation and Management of the Housing Affordability Fund
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.12 2011–12
Implementation of the National Partnership Agreement on Remote Indigenous Housing in the Northern Territory
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.13 2011–12
Tasmanian Freight Equalisation Scheme
Department of Infrastructure and Transport
Department of Human Services

ANAO Audit Report No.14 2011–12
Indigenous Protected Areas
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.15 2011–12
Risk Management in the Processing of Sea and Air Cargo Imports
Australian Customs and Border Protection Service

ANAO Audit Report No.16 2011–12
The Management of Compliance in the Small to Medium Enterprises Market
Australian Taxation Office

ANAO Audit Report No.17 2011–12
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2011

ANAO Audit Report No.18 2011–12
Information and Communications Technology Security: Management of Portable Storage Devices

ANAO Audit Report No.19 2011–12
Oversight and Management of Defence's Information and Communication Technology
Department of Defence

ANAO Audit Report No.20 2011–12
2010–11 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.21 2011–12
Administration of Grant Reporting Obligations
Department of Finance and Deregulation

ANAO Audit Report No.22 2011–12
Administration of the Gateway Review Process
Department of Finance and Deregulation

ANAO Audit Report No.23 2011–12
Administration of the National Greenhouse and Energy Reporting Scheme
Department of Climate Change and Energy Efficiency

ANAO Audit Report No.24 2011–12
Administration of Government Advertising Arrangements: March 2010 to August 2011

ANAO Audit Report No.25 2011–12
Administration of Project Wickenby
Australian Taxation Office
Australian Crime Commission
Australian Federal Police

ANAO Audit Report No.26 2011–12
Capacity Development for Indigenous Service Delivery
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment, and Workplace Relations
Department of Health and Ageing

ANAO Audit Report No.27 2011–12
Establishment, Implementation and Administration of the Bike Paths Component of the Local Jobs Stream of the Jobs Fund
Department of Regional Australia, Local Government, Arts and Sport
Department of Infrastructure and Transport

ANAO Audit Report No.28 2011–12
Quality On Line Control for Centrelink Payments
Department of Human Services

ANAO Audit Report No.29 2011–12
Administration of the Australia Network Tender Process
Department of Foreign Affairs and Trade
Department of Broadband, Communications and the Digital Economy
Department of the Prime Minister and Cabinet

ANAO Audit Report No.30 2011–12
Fighting Terrorism at its Source
Australian Federal Police

ANAO Audit Report No.31 2011–12
Establishment and Use of Procurement Panels
Australian Securities and Investments Commission
Department of Broadband, Communications and the Digital Economy
Department of Foreign Affairs and Trade

ANAO Audit Report No.32 2011–12
Management of Complaints and Other Feedback by the Department of Veterans' Affairs
Department of Veterans' Affairs

ANAO Audit Report No.33 2011–12
Management of ePassports
Department of Foreign Affairs and Trade

ANAO Audit Report No.34 2011–12
Upgrade of the M113 Fleet of Armoured Vehicles
Department of Defence
Defence Materiel Organisation

ANAO Audit Report No.35 2011–12
Indigenous Early Childhood Development. New Directions: Mothers and Babies Services
Department of Health and Ageing

ANAO Audit Report No.36 2011–12
Development and Approval of Grant Program Guidelines
Department of Finance and Deregulation

ANAO Audit Report No.37 2011–12
The Child Support Program's Management of Feedback
Department of Human Services

ANAO Audit Report No.38 2011–12
Administration of the Private Irrigation Infrastructure Operators Program in New South Wales
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.39 2011–12
Management of the National Solar Schools Program
Department of Climate Change and Energy Efficiency

ANAO Audit Report No.40 2011–12
Interpretative Assistance for Self Managed Superannuation Funds
Australian Taxation Office

ANAO Audit Report No.41 2011–12
National Partnership Agreement on Literacy and Numeracy
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.42 2011–12
Management of the Multicultural Servicing Strategy for the delivery of Centerlink Services
Department of Human Services

ANAO Audit Report No.43 2011–12
National Partnership Agreement on Remote Service Delivery
Department of Families, Housing, Community Service and Indigenous Affairs

ANAO Audit Report No.44 2011–12
Administration of the Primary Care Infrastructure Grants Program
Department of Health and Ageing

ANAO Audit Report No.45 2011–12
Administration of the Health and Hospitals Fund
Department of Health and Ageing

ANAO Audit Report No.46 2011–12
Administration of Northern Australia Quarantine Strategy
Department of Agriculture, Fisheries and Forestry

ANAO Audit Report No.47 2011–12
Small Business Superannuation Clearing House
Department of the Treasury
Department of Human Services
Australian Taxation Office

ANAO Audit Report No.48 2011–12
Administration of Mental Health Initiatives to Support Younger Veterans
Department of Veterans' Affairs

Current Better Practice Guides

The following Better Practice Guides are available on the ANAO website.

Public Sector Environmental Management	Apr 2012
Developing and Managing Contracts – Getting the right outcome, achieving value for money	Feb 2012
Public Sector Audit Committees	Aug 2011
Human Resource Information Systems Risks and Controls	Mar 2011
Fraud Control in Australian Government Entities	Mar 2011
Strategic and Operational Management of Assets by Public Sector Entities – Delivering agreed outcomes through an efficient and optimal asset base	Sep 2010
Implementing Better Practice Grants Administration	Jun 2010
Planning and Approving Projects – an Executive Perspective	Jun 2010
Innovation in the Public Sector – Enabling Better Performance, Driving New Directions	Dec 2009
SAP ECC 6.0 – Security and Control	Jun 2009
Preparation of Financial Statements by Public Sector Entities	Jun 2009
Business Continuity Management – Building resilience in public sector entities	Jun 2009
Developing and Managing Internal Budgets	Jun 2008
Agency Management of Parliamentary Workflow	May 2008
Public Sector Internal Audit – An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions – Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts – Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives – Making implementation matter	Oct 2006