



Australian Government
Department of Home Affairs



Department of Home Affairs submission to the Inquiry into Expansion of ACLEI's jurisdiction and the corruption vulnerabilities of law enforcement agencies' contracted services

Parliamentary Joint Committee on the Australian
Commission for Law Enforcement Integrity

12 October 2021

Table of Contents

Department of Home Affairs submission to the Inquiry into Expansion of ACLEI's jurisdiction and the corruption vulnerabilities of law enforcement agencies' contracted services	1
Table of Contents	2
Introduction	3
Response to Terms of Reference	3

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity (PJCALEI) inquiry into the expansion of ACLEI's jurisdiction and the corruption vulnerabilities of law enforcement agencies' contracted services.
2. The Department, including the Australian Border Force (ABF), contributes to Australia's Prosperity, Security and Unity by delivering critical services that the Australian public, industry and international stakeholders rely on.
3. The Department is responsible for centrally coordinated strategy and policy leadership in relation to immigration, citizenship and multicultural affairs, domestic and national security arrangements, law enforcement, emergency management, counter-terrorism, social cohesion, the protection of Australia's sovereignty, the integrity of the border, and the resilience of national infrastructure.
4. The ABF is an operationally independent body responsible for implementing Australia's border enforcement policies, managing frontline border law enforcement, customs and immigration detention related activities to protect the integrity of Australia's borders. The ABF facilitates movements of legitimate trade and travel across Australia's borders.

Response to Terms of Reference

A: The January 2021 expansion of ACLEI's jurisdiction from five to nine law enforcement agencies, including the support given to, and effectiveness of, agencies undertaking new responsibilities in working collaboratively with ACLEI in detecting, investigating and preventing corruption.

5. As the Department was already operating under ACLEI jurisdiction in accordance with the *Law Enforcement Integrity Commissioner Act 2006* (LEIC Act), the Department was not impacted by the expanded ACLEI jurisdiction in January 2021.
6. The Department and ACLEI have a strong integrity partnership, which supports the Integrity Commissioner in carrying out her responsibilities to detect, investigate and prevent corrupt conduct in Australian Government agencies with law enforcement functions. Where corruption issues arise, the Department works closely with ACLEI, including on any joint investigations.
7. The Department's Integrity and Professional Standards Branch (I&PS) is responsible for receiving, triaging and assessing all allegations that relate to serious misconduct, corrupt conduct and criminal conduct. From 1 July 2020 to 30 June 2021, I&PS:
 - Received 701 integrity referrals, and
 - Notified 279 matters to the Integrity Commissioner, as the matter raised a potential corruption issue.
8. Matters commonly referred to the Integrity Commissioner by the Department include alleged repeated unauthorised access to departmental systems, bribery for favourable immigration outcomes and other abuse of office allegations, including provision of information or assistance to import prohibited items for a benefit.
9. The Department welcomes an expanded ACLEI jurisdiction, and in future, supports the establishment of the Commonwealth Integrity Commission (CIC) to enable and assist with investigations of suspected corrupt activity across the APS.

B: The additional corruption vulnerabilities that may exist from the contracting of services or functions by law enforcement agencies to external service providers.

10. Corruption vulnerabilities exist where individuals are provided non-public access to the Department's staff, information, equipment, premises and assets. The contracting of services or functions to external parties may give rise to additional corruption risks, for example where personnel employment screening processes differ to that of the Department's standards—including where sub-contracting may occur, or where service providers utilise own systems which may impede the Department's ability to monitor or audit for potential corruption risk.
11. To address corruption risks posed by contracted services, the Department has in place fraud and corruption control mechanisms and robust Integrity and Professional Standards Frameworks (the Frameworks).

Fraud and corruption control

12. The Department and the ABF's Fraud Control Plans outline our commitment to effectively manage and mitigate fraud and corruption in the Department and the ABF. The Plans describe key mechanisms to prevent, detect, respond, monitor, evaluate and report on fraud and corruption risks. Further, the Department is required to conduct Fraud and Corruption Risk Assessments (FCRAs) regularly and where there is substantial changes in structure, functions or activities. FCRAs are required to be reviewed at least every two years.
13. Regarding procurement processes, which seek to engage contracted services, mandatory fraud clauses may differ depending on the type of procurement. For example, open approaches to market by the Department requires tenderers set out a Risk Management and Fraud Control Plan, and how they will identify, prevent and report and manage risk in relation to fraud in the delivery of the requirement. Departmental contracts include mandatory clauses that outline that the supplier must comply with relevant fraud and anti-corruption frameworks, as well as the Commonwealth Fraud Control Framework.

Integrity and Professional Standards Frameworks

14. All Immigration and Border Protection (IBP) workers must abide by the Department's Frameworks. The Frameworks set the standards of behaviour that underpin a high performance and professional organisational culture.
 - IBP workers are defined by section 4 of the *Australian Border Force Act 2015* (Cth) and related Secretary Determinations (and in particular the Secretary's Determination of Immigration and Border Protection Workers – see <https://www.homeaffairs.gov.au/commitments/files/determination-workers.pdf>)
15. The Professional Standards Framework is an overarching framework encompassing guidelines from the Australian Public Service Commission, including obligations contained in the PS Act like the APS Code of Conduct, the APS Values and APS Employment Principles, as well as the Integrity Framework, and number of Secretary's Determinations and Directions.
16. The Integrity Framework is a component of the Professional Standards Framework and comprises a series of measures that are designed to protect the Department's people, property, systems and information from infiltration and corruption.
17. This includes, for example, a requirement for IBP workers to hold and maintain an Employment Suitability Clearance issued by the Department, and a minimum Baseline security clearance issued by the Australian Government Security Vetting Agency. IBP workers are also subject to drug and alcohol testing, must report changes in their circumstances or associations, and mandatorily report any serious misconduct, corrupt conduct or criminal activity about themselves or other IBP workers. Collectively, the Frameworks reinforce a workplace culture that does not ignore corruption.

18. While contracted personnel and external service providers who work 'in house' are generally considered to be IBP workers, the Department has adopted a risk-based approach to managing external service providers who work offsite. In particular, persons who are engaged as external service providers but who work offsite are only considered to be an IBP worker (and therefore subject to the Integrity Framework) if they have 'non-public access' to the Department's resources such as its ICT network, information or assets. For example individuals providing services to the Department as a health practitioner are excluded from the definition of an IBP worker under the abovementioned Secretary Determination.
19. In the event that the Department identifies a non-IBP worker engaging in corrupt activity or inappropriate behaviour, the Department currently deals with the matter under the contractual arrangements governing that individual's engagement and/or by referring the matter to police.
20. While the Department's Integrity Framework applies to those external service providers deemed to be IBP workers, these individuals may not be considered 'staff members' for the purposes of the LEIC Act, and therefore are generally not subject to ACLEI's jurisdiction. There are however, certain exceptions. For example, individuals performing certain roles in the Immigration Detention Network (such as the Department's Facilities and Detainee Service Provider, Serco) are considered to be 'staff members' by virtue of section 10(2A)(e) of the LEIC Act.
21. The establishment of the CIC provides an opportunity to streamline inconsistencies where a person may be considered an IBP worker, but is not subject to ACLEI's (or in future, the CIC's) jurisdiction, or vice versa.

Overview of the Department's contracted services

22. The Department uses contracted service providers to support a broad range of administrative and operational functions which can be attributed broadly, for the purpose of this submission, to four main categories:
 - border services,
 - immigration detention services,
 - Information and Communications Technology (ICT) services, and
 - non-ICT/Other services (described under each heading below).

Border services

23. Border services include trade and travel facilitation and modernisation, and effective customs, immigration (including visa and citizenship processing), maritime functions, and enforcement activities across the border continuum.
24. Examples of contracted services in relation to this function include:
 - Contracted resources via established whole-of-government panels to provide specialist expertise to support our trade and traveller modernisation initiatives, including supporting the Government's Simplified Trade System reform and the National Plan to transition Australia's National COVID Response. These resources undertake support functions such as project/program management, business analysis, strategic advice and the development of traveller, trade and customs modernisation initiatives.
 - Contracted resources to provide unpack/repack services in support of the ABF's cargo examination function. In order to support the service they provide, unpack/repack contracted personnel are provided an awareness of cargo targeted in the examination process. Contracted personnel may develop an understanding of sensitive ABF operational procedures and patterns, and may have an opportunity to misuse this information.
 - High value/high risk contracts with several airline providers who undertake domestic and international chartered operations, as well as maritime surveillance activity.

- Contracts with commercial partners to deliver services at Australian Visa Application Centres and Australian Biometric Collection Centres overseas. Service delivery partners provide administrative services including information services, visa lodgement and biometric enrolment services. Service delivery partner staff do not make visa decisions, and operate on a user-pays basis, with visa applicants paying for the cost of the service. Applications are provided to the Department for processing.
- Engagement of services to support visa processing—The Department's workforce includes Locally Engaged Employees (LEEs) based within its offshore network to support immigration services. LEEs are not directly engaged by the Department but instead are generally engaged by the Department of Foreign Affairs and Trade (DFAT) under a contract for services. LEEs may also be engaged by DFAT under section 74 of the *Public Service Act 1999* (Cth) (PS Act). As a consequence of their engagement, there is no direct employment contract between LEEs and the Department.

Immigration detention services

25. The Department uses contracted service providers to support operational functions including health and garrison services for the delivery of a safe, secure and sustainable Immigration Detention Network (IDN).
26. The Department's Facilities and Detainee Service Provider, Serco, are considered IBP workers for the purpose of the Integrity Framework. However, only certain categories of Serco officers are within ACLEI jurisdiction—those declared by the Minister to be 'officers' for the purposes of subsection 5(1) of the *Migration Act 1958* (Cth) (Migration Act)—see section 10(2A)(e) of the LEIC Act.

ICT services

27. ICT services include a range of technology functions, ranging from the procurement of small scale software and hardware, through to providing individual contractors to support the development of new IT systems or maintaining existing systems, as well as complex service contracts for major ICT capabilities (including hosting and managing critical data processing and storage systems, data networks, and 'in the field' ICT support services).
28. Additional corruption risks associated with contracted ICT functions may arise from those seeking to obtain financial benefit, through potential undue influence on associated procurements or recruitment processes. Additionally, the privileged system access that some ICT contractors and External Service Provider Personnel are provided with, to enable them to manage and maintain systems, may give rise to data integrity risks.
29. By way of scale, the Department currently engages approximately 1,350 external personnel in corporate ICT functions (consisting of around 500 contractors and 850 External Service Provider Personnel). In addition, the Department expends approximately \$500m per annum through ICT contracts (including contractors)—this covers ICT services, software, and hardware acquired with both Operating and Capital funds. The Department's 20 strategic and critical ICT services contracts are collectively worth over \$2.5b (funded from both Operating and Capital funds).

Non-ICT/Other services

30. Non-ICT and Other services include a range of corporate support and enabling functions, such as security guarding, property services, translating services, physical and digital records services and mail, freight and courier services.
31. Examples of contracted services in relation to this function include:
 - The Department uses a contracted service provider for security guarding services across its sites nationally. The primary role of security guards is to screen staff and visitor/contractor access to secure office areas and to monitor the public areas for the purpose of protecting the Department's staff, information, equipment, premises and assets. Each of the premises is guarded in accordance with the contract and requirements specific to each of the sites.

- Client enquiries, for example in relation to travel, trade and bringing goods in and out of Australia, are managed by a contracted service provide through the Department's global service centre.
32. The Department may also engage consultancy services that cut across the categories outlined. The Department's policy for selecting and engaging consultants is based on the core principle of value for money, and is conducted in accordance with the *Public Governance, Performance and Accountability Act 2013* (Cth) and the Commonwealth Procurement Rules. Decisions to procure consultancy services are made both strategically and operationally; injecting specialist skills, knowledge and independent expertise in areas outside of the Department's core business functions.

C: What systems or processes are in place within law enforcement agencies to identify, report and investigate potential corruption within external service providers.

33. The Department occupies a position of trust, and our service to the Australian community is guided by the values of integrity, professionalism, respect and accountability.
34. The Department's integrity model focuses on prevention and proactive early intervention to deter, detect and correct behaviours. The Department leverages technical capability to actively identify potential high-risk behaviours, and disrupt inappropriate conduct. For example through the Department's Integrity Active Detection Program which seeks to identify potential misuse of departmental systems, and disrupt behaviour and prevent more serious potential misconduct.
35. Staff, contractors and members of the public can report integrity and corruption matters in relation to the Department in a number of ways. For example:
- Directly to I&PS via phone, email, online and in person
 - Through Border Watch via online reporting, phone and email
 - Through the Public Interest Disclosure Scheme, and
 - Directly to ACLEI or other law enforcement partners.
36. Where contractors are considered IBP workers, corruption risks are identified and managed through the Department's Integrity Frameworks, including through security clearances, personnel suitability assessments, mandatory reporting and other integrity obligations.
37. Allegations of corruption involving an external service provider are currently dealt with on a case-by-case basis depending on the specific circumstances of the external service provider. Where that individual is subject to ACLEI's jurisdiction, the corruption issue relating to that individual will be referred to ACLEI under the LEIC Act.
38. Where an individual is not subject to ACLEI's jurisdiction, the Department will generally deal with the matter under the contractual arrangements between the Department and the external service provider governing the individual and/or by referring the matter to police.
39. The Department notes that the establishment of the CIC offers an opportunity to promote greater consistency in how corruption issues involving external service providers are investigated and will enable the specialist investigative capabilities possessed by the proposed CIC to be used to support these processes.
40. Systems and processes in place to identify, report and investigate potential corruption in the Department's four main categories of contracted services are described further below.

Border services

41. Contractors engaged through modernisation initiatives and for unpack/repack services for the ABF are considered IBP workers for the purposes of the Department's Integrity Frameworks.
42. LEEs are considered IBP workers and are subject to ACLEI's jurisdiction under the LEIC Act as they have been declared by the Minister to be 'officers' for the purposes of subsection 5(1) of the Migration Act—see section 10(2A)(e) of the LEIC Act.

Immigration detention services

43. Service providers working in the IDN are contractually bound to a risk based performance management framework. This framework captures failings of contracted service provider personnel against the Code of Conduct (including matters of corruption) and applies a financial abatement if confirmed. Contracted service providers are required to undertake pre-employment checks (including police checks) and include Code of Conduct in the induction course prior to delivering services in an immigration detention facility.
44. The ABF monitors immigration detention contracted service providers' performance in situ through regular governance forums and monthly performance reporting, as well as incident reporting and mandatory reviews of critical incidents. The Department, including the ABF, regularly conducts its own internal assurance reviews of issues, including functions delivered by contractors.
45. There are main avenues of identifying potential issues including:
 - Self-reporting by the service provider
 - Monitoring and observation by ABF officers
 - Detainee complaints, and
 - Suspicious activity reported to the ABF by scrutiny bodies or members of the public.
46. Various bodies such as Comcare, the Commonwealth Ombudsman, the Australian Human Rights Commission and Australian Red Cross also provide a level of independent assurance over immigration detention and regularly conduct their own investigations and/or reports on issues in immigration detention.

ICT services

47. Due to the diverse nature of the Department's contracted ICT services (ranging from small software licence purchases, to large-scale externally managed data processing services) the corruption control measures are also equally diverse.
48. Where ICT services are provided through a company (rather than individual contractors) the relevant contracts require the service provider to comply with all relevant Commonwealth security policies, including those covering integrity and professional standards risks. Any breaches of those policies and obligations are required to be reported to the Department and any other relevant authorities, and are notifiable to ACLEI if within jurisdiction.

Non-ICT/Other services

49. Due to the diverse nature of contracted services in this category, some contractors may have additional requirements to abide by codes of conduct relevant to their qualification or accreditation. For example, in relation to contracted translation services; interpreters are also bound by the Australian Institute of Interpreters and Translators Inc. Code of Conduct and Code of Ethics. Where misconduct occurs, breaches may be subject to internal investigation by the service provider, TIS National.

D: Whether there are similar corruption vulnerabilities in partnerships between law enforcement agencies and other government agencies who are not subject to ACLEI's powers for investigation.

50. The Department maintains close working relationships with other Home Affairs Portfolio agencies, law enforcement partners, and other government agencies. A number of these key agency partners are already operating within the ACLEI jurisdiction, for example, the Australian Federal Police, and more recently, the Australian Tax Office.
51. Of those agencies that are not within ACLEI jurisdiction, the majority of those agencies the department works with have internal anti-corruption mechanisms and other forms of corruption oversight, including for example, State and Territory Police.
52. Additional Government frameworks also support agencies in managing protective security more broadly, including through the Protective Security Policy Framework.

53. As the Department is within ACLEI jurisdiction, the LEIC Act remains the key mechanism for reporting potential corruption issues to ACLEI for investigation, through mandatory reporting of both significant and non-significant corruption matters. The LEIC Act informs the subsequent action by the Department, including the way in which the Department can address issues identified. The Department's Section 17 Agreement with ACLEI outlines what is considered non-significant corruption, within the scope of the LEIC Act.
54. The Department notes that the corruption risk from our interaction with agencies that are not within the ACLEI jurisdiction is low, but welcomes an expanded ACLEI jurisdiction, and in future, the establishment of the CIC to address potential or suspected corrupt activity across the APS.

E: Any other relevant matter

55. The Department notes recent media reporting in relation to aviation and maritime security that may be relevant to the Terms of Reference for this Inquiry.

Aviation and maritime security

56. The Department is committed to working closely with the transport sector on a range of security and safety matters to ensure Australia's aviation and maritime environments are safe and secure.
57. The aviation and maritime security identification card (ASIC and MSIC) schemes are an important part of securing the aviation and maritime sectors and ensure that anyone who requires unescorted access to the secure areas of security regulated airports or security regulated ports and offshore facilities are subject to a background check.
58. While ASICs and MSICs have successfully deterred unlawful interference and terrorism, several parliamentary inquiries have identified the schemes' limited scope and recommended that they be expanded to protect airports, seaports and offshore facilities against exploitation by serious criminals. Australia's transport sector remains an attractive target for terrorists and serious criminal organisations.
59. Based on intelligence from 2019, the Australian Criminal Intelligence Commission (ACIC) has identified approximately 227 ASIC or MSIC holders who are currently recorded on the ACIC's national criminal intelligence target lists.
60. Recent developments, such as Operation IRONSIDE and Project Brunello, demonstrate the threat of organised crime groups and their ability to infiltrate the aviation and maritime sectors.
61. The passage of the *Transport Security Amendment (Serious Crime) Act 2021* (Cth) strengthens the ASIC and MSIC schemes by:
- creating an additional purpose to prevent the use of aviation and maritime transport and offshore facilities in connection with serious crime;
 - establishing the regulatory framework for introducing new criteria to target serious criminal offences; and
 - introducing criminal intelligence assessments into the background checking process.
62. On 23 August 2021, the new criteria affecting eligibility came into effect via the *Transport Security Legislation Amendment (Serious Crime) Regulations 2021* (Cth), which ensures that people with serious criminal convictions will be ineligible to hold an ASIC or MSIC.
- The amendments introduced new criteria affecting eligibility to hold or be issued a card targeting serious criminal offences, listing offences such as those relating to involvement with a criminal organisation or gang, dealing with proceeds of crime and the sexual exploitation of a child.

63. In the coming year, the Department and the ACIC will further strengthen the ASIC and MSIC schemes by implementing criminal intelligence assessments into the ASIC and MSIC background check.

- In future, where the ACIC identifies links between an ASIC or MSIC holder or applicant and serious and organised crime, a careful evaluation will be undertaken to determine if intelligence or information suggests the individual may commit a serious and organised crime or assist another person to commit a serious and organised crime.
- If the level of risk meets this threshold, the ACIC may issue an adverse criminal intelligence assessment which prevents an individual from holding (or being issued) an ASIC or MSIC.
- The implementation of the *Transport Security Amendment (Serious Crime) Act 2021* (Cth) will significantly impede the ability of anyone connected to serious crime to hold an ASIC or MSIC and physically access secure zones of airports, ports and offshore oil and gas facilities.

64. The Department will continue to work with industry to address identified vulnerabilities and strengthen aviation and maritime security against security and criminal threats.