Australian Government
Australian Commission for Law Enforcement Integrity

Investigation Report – Operation Chandra

Operation Chandra – An investigation into allegations of corrupt conduct involving Locally Engaged Employees at the Australian Embassy in Phnom Penh, Cambodia.

OFFICIAL

A report to the Attorney-General, prepared under section 54 of the *Law Enforcement Integrity Commissioner Act 2006* (Cth)

---

aclei.gov.au

Enquiries about this report can be directed to the
Australian Commission for Law Enforcement Integrity
GPO Box 605, Canberra, ACT, 2601
or by email to contact@aclei.gov.au

Investigation Reports published by the Integrity Commissioner and summaries of reports which have not been made public can be found on the ACLEI website: aclei.gov.au

© Commonwealth of Australia 2022

Except for the Commonwealth Coat of Arms, the Australian Commission for Law Enforcement Integrity logo and any material protected by a trade mark, this document is licenced by the Commonwealth of Australia under the terms of a Creative Commons Attribution 3.0 Australia licence (www.creativecommons.org/licenses/by/3.0/legalcode).

You are free to copy, communicate and adapt the work, as long as you attribute the document to the Australian Commission for Law Enforcement Integrity and abide by the other terms of the licence.

This publication should be attributed as:

> Operation Chandra— An investigation into allegations of corrupt conduct involving Locally Engaged Employees at the Australian Embassy in Phnom Penh, Cambodia.

Australian Commission for Law Enforcement Integrity, Canberra.

The terms under which the coat of arms may be used can be found at:
www.dpmc.gov.au/government/commonwealth-coat-arms

Contents

About ACLEI Reports

The Law Enforcement Integrity Commissioner Act

1. The *Law Enforcement Integrity Commissioner Act 2006* (Cth) (LEIC Act) establishes the office of Integrity Commissioner, supported by a statutory agency, the Australian Commission for Law Enforcement Integrity (ACLEI).

The role of the Integrity Commissioner and ACLEI

2. The role of the Integrity Commissioner and ACLEI is to detect and prevent corrupt conduct and deal with corruption issues in designated agencies—presently the:
    - Australian Criminal Intelligence Commission (including the former Australian Crime Commission, the former National Crime Authority and the former CrimTrac Agency);
    - Australian Federal Police (including ACT Policing);
    - Australian Transaction Reports and Analysis Centre (AUSTRAC); and
    - Department of Home Affairs (including the Australian Border Force).
3. Other Australian Government agencies with law enforcement functions may be prescribed by regulation as being within the jurisdiction of the Integrity Commissioner.[1] At present those agencies include prescribed aspects of the:
    - Department of Agriculture, Water and the Environment (DAWE)
    - Australian Competition and Consumer Commission (ACCC)
    - Australian Prudential Regulation Authority (APRA)
    - Australian Securities and Investment Commission (ASIC);
    - Australian Taxation Office (ATO); and
    - Office of the Special Investigator (OSI).

Corrupt conduct

4. A staff member of a law enforcement agency 'engages in corrupt conduct' if the staff member:
    - abuses his or her office
    - perverts the course of justice, or
    - having regard to his or her duties and powers, engages in corrupt conduct of any other kind.
5. The Integrity Commissioner is to give priority to dealing with serious and systemic corruption.[2]

---

1 Law Enforcement Integrity Commissioner Act 2006 (Cth) s 5(1) (definition of 'law enforcement agency') (LEIC Act); Law Enforcement Integrity Commissioner Regulations 2017 (Cth) s 7.

2 Ibid s 6(1).

Dealing with corruption issues

6. A corruption investigation can commence in different ways:

   - the Minister may refer to the Integrity Commissioner an allegation or information that raises a corruption issue.
   - the head of a law enforcement agency within ACLEI's jurisdiction must notify the Integrity Commissioner of any allegation or information that raises a corruption issue which relates to that agency.
   - any person or government agency can refer to the Integrity Commissioner an allegation or information that raises a corruption issue. A referral may be anonymous, or on behalf of another person.
   - the Integrity Commissioner can commence an investigation on his or her own initiative.[3]

7. The Integrity Commissioner may decide to deal with the corruption issue in a number of ways:

   - have ACLEI investigate the corruption issue either alone or jointly with another government agency or an integrity agency for a State or Territory.
   - refer the corruption issue to the law enforcement agency to conduct its own investigation.
   - decide that an investigation is not warranted.

8. The Integrity Commissioner can decide to manage or oversee any investigation that has been referred to a law enforcement agency. If the law enforcement agency were not the Australian Federal Police (AFP), the Integrity Commissioner can also refer the issue to the AFP for investigation and may manage or oversee that investigation.[4]

Reports

9. After completing a corruption investigation, the Integrity Commissioner must prepare a report setting out:

   a. the Integrity Commissioner's findings on the corruption issue; and

   b. the evidence and other material on which those findings are based; and

   c. any action that the Integrity Commissioner has taken, or proposes to take, under Part 10 in relation to the investigation; and

   d. any recommendations that the Integrity Commissioner thinks fit to make and, if recommendations are made, the reasons for those recommendations.[5]

10. The Integrity Commissioner must give the report on the investigation to the Minister who administers the LEIC Act and a copy to the head of the law enforcement agency to which the corruption issue relates.[6]

---

[3] Ibid ss 18–24 and 38.

[4] Ibid ss 26–30.

[5] Ibid ss 54(1)–(2).

[6] Ibid s 55.

Standard of proof

11. The Integrity Commissioner makes findings about whether a person has engaged in corrupt conduct, based on the balance of probabilities. Those findings may not be the same as those that would be made by a court deciding on criminal guilt beyond a reasonable doubt.

12. Before making a finding, the Integrity Commissioner is required to be 'reasonably satisfied', based on relevant facts, that the corrupt conduct occurred and that the corrupt conduct was within the meaning of the LEIC Act.

13. In considering whether or not the Integrity Commissioner is 'reasonably satisfied' of relevant facts, the Integrity Commissioner applies the reasoning set out in *Briginshaw v Briginshaw,*[7] *Rejfek v McElroy,*[8] *and Re Day.*[9]

[7] (1938) 60 CLR 336, 361–62 (Dixon J).
[8] (1965) 112 CLR 517, 521.
[9] (2017) 91 ALJR 262, 268 [14]–[18].

Preface to the public version of Investigation Report

14. This Investigation Report is a report on Operation Chandra, a corruption investigation relating to locally engaged employees at the Australian High Commission in Phnom Penh, Cambodia.

15. Operation Chandra commenced in December 2018 and considered allegations that two locally engaged employees were engaging in corrupt conduct by improperly disclosing information relating to visa applications.

16. The investigation resulted in findings of corrupt conduct against both employees.

17. Following this, I prepared my report on Operation Chandra pursuant to s 54 of the LEIC Act. I consulted with the relevant parties in accordance with the procedural fairness requirements under s 51 of the LEIC Act, prior to the finalisation of my report.

18. On 23 December 2021, I provided my finalised report on Operation Chandra to the Attorney-General and the Secretary of the Department of Home Affairs (Home Affairs) in accordance with s 55 of the LEIC Act.

19. I then considered whether it was in the public interest to publish the report on Operation Chandra under s 209 of the LEIC Act. In recognition of my corruption findings in Operation Chandra, I was satisfied that my report contained opinions or findings that could be considered critical of both persons of interest. As such, I provided them with a copy of the report an opportunity to be heard prior to making a decision on whether to publish this report in accordance with s 210 of the LEIC Act. This process concluded on 13 April 2022.

20. On 14 February 2022, I notified the Secretary of Home Affairs that I was considering publishing the report on Operation Chandra and provided the department with the opportunity to make any submissions on the proposed publication. The process concluded on 11 March 2022.

21. Accordingly, this is the version of Investigation Report for Operation Chandra I have decided is in the public interest to disclose.

Jaala Hinchcliffe
Integrity Commissioner
9 June 2022

Summary of the Investigation

Notification

Imposter immigration email address

22. On 1 November 2018 the Australian Embassy in Phnom Penh (Phnom Penh Post) informed ACLEI that it suspected an unknown locally engaged employee (LEE) had created an imposter immigration email address and was using it to contact a visa applicant about their application.

Officer K

23. On 26 November 2018, the Secretary of the Department of Home Affairs (Home Affairs) notified the then Integrity Commissioner, Mr Michael Griffin AM, of a corruption issue pursuant to s 19(1) of the LEIC Act.

24. The notification alleged that a LEE, Officer K, who worked as an Enforcement and Engagement Officer based Phnom Penh Post, was improperly disclosing information relating to the status of visa applications, without a work-related need, in exchange for money.

Jurisdiction

25. On 11 December 2018, the then Integrity Commissioner decided to investigate the notification regarding Officer K pursuant to s 26(1)(a) of the LEIC Act. The corruption investigation was named 'Operation Chandra'. The then Integrity Commissioner was satisfied:

    a. the allegations were within ACLEI's jurisdiction because LEEs of Australian overseas posts were considered staff members of Home Affairs, a law enforcement agency;

    b. the person identified in the notification, Officer K, was a LEE; and

    c. the allegations fell within the meaning of a 'corruption issue' as defined by s 7 of the LEIC Act. The information raised an issue about whether one or more staff members in the Australian Embassy had used their position to influence the processing of visas for financial benefit. The former Integrity Commissioner was satisfied that, if such conduct was engaged in by a staff member of Home Affairs, that staff member may have 'engaged in corrupt conduct' pursuant to s 6 of the LEIC Act.

26. At the time of notification, it was unknown whether Officer K was involved in the allegations relating to the imposter immigration email address. Given the similarity of the two allegations, the imposter email allegation was investigated as part of Operation Chandra.

27. On 6 February 2019, the former Integrity Commissioner reconsidered how to deal with this matter pursuant to s 42 of the LEIC Act and decided to investigate this matter jointly with Home Affairs and the Department of Foreign Affairs and Trade (DFAT), pursuant to ss 26(1)(a) and 26(2) of the LEIC Act.

28. On 6 March 2019, ACLEI investigators were appointed by the Ambassador to the Kingdom of Cambodia to investigate the allegations and determine whether the LEEs involved in the allegations had breached the LEE Code of Conduct.

Background

Onshore and offshore visa processing

29. Home Affairs processes visa applications both onshore and offshore. Offshore processing takes place at diplomatic posts operated by the Department of Foreign Affairs and Trade (DFAT). Offshore processing is undertaken by a mix of Australian-based (A-based) staff and LEEs.

30. A-based staff have responsibility of managing the visa processing function and supervising visa processing staff at post. At the time the allegations were made, the A-based staff were comprised of Principal Migration Officers (PMO) and Senior Migration Officers (SMO).[10]

31. Locally engaged employees (LEEs) perform the bulk of visa processing at post under the supervision of A-based staff. Their authorisation to make decisions about visa applications was limited to certain LEE roles and duties and decisions about permanent visas were restricted to A-based staff or expatriate LEEs.

32. LEEs are formally engaged by DFAT to work at the diplomatic post[11] and are assigned to the Home Affairs section of post. As such, LEEs are considered staff members of Home Affairs for the purposes of the LEIC Act.

33. LEEs are subject to various employment conditions, including a Code of Conduct.[12]

Investigation

Allegations involving Officer K

34. On 18 October 2018, a SMO at the Phnom Penh Post discovered an unlocked mobile phone ringing under the work station of Officer K ('located phone') after business hours. The located phone was an older model LG Triple Sim device branded "Tri Sim 3". The SMO considered the located phone to be suspicious, as it appeared to be hidden and it was an older phone model than Officer K was known to possess. The SMO recalled Officer K carrying two smart phones, one being their personal and the other being work issued.

35. Upon opening the message inbox, the SMO observed incoming text messages which:

    a. contained the details of visa applicants and applications;

    b. requested assistance with looking up the status of these applications;

---

[10] During the course of the investigation, there were three Immigration Programs Division A-based role types at Overseas Posts: the EL2 Chief Migration Officer (CMO), the EL1 Principal Migration Officer (PMO) and the APS 6 Senior Migration Officer (SMO). Only two of these positions were present at Home Affairs office in Phnom Penh post – a PMO and an SMO. In 2021, these roles are generally referred to by their diplomatic classification: Counsellor (Immigration and Border Protection), First Secretary (Immigration and Border Protection) and Second Secretary (Immigration and Border Protection).

[11] Subsection 74(1) of the *Public Service Act 1999* (Cth) permits an Agency Head, on behalf of the Commonwealth, to engage persons overseas to perform duties overseas as employees. However, such a person is not an 'Australian Public Service (APS) employee' under that Act: s 7(1) definition of 'APS employee'.

[12] This code of conduct outlines a general expectation that LEEs uphold the same standards of conduct, honest, and integrity as that expected of APS employees while also specifying job-relevant standards.

c. discussed the payment of money;

d. were dated between 2014 to September 2018;

e. were sometimes addressed to a known nickname for Officer K; and

f. were from both Australian and Cambodian contact numbers.

36. The SMO observed outgoing text messages from the located phone which:

a. disclosed the status of visa applications;

b. discussed the receipt of money; and

c. requested contacts to send emails to a non-government email address.

37. After discovering the text messages on the located phone, the SMO photographed a small portion of the messages and the missed call list before returning the located phone to its original location. The same evening, the SMO notified the PMO at Phnom Penh Post about the discovery of the located phone. The following day, the PMO notified I&PS.

Officer K

38. At the time of notification, Officer K had been employed as a LEE with Phnom Penh Post for approximately 10 years. Officer K had had various roles during that time and in 2018 was an Enforcement and Engagement Officer.

39. Departmental records confirm that Officer K had undertaken regular mandatory training. From June 2012 to October 2018, Officer K had undertaken at least 23 training courses and assessments relating to integrity.

40. In addition to integrity training, Officer K signed the following documents during the course of their employment with Home Affairs:

a. a Disclosure of Private, Financial and Other Interests form in 2019 declaring that neither they nor a member of their immediate family had any personal, financial or other interests that could or could be seen to influence their decisions or actions in connection with their official duties. Further, by signing the declaration, they declared that they had read DFAT's policy regarding conflicts of interest and they were aware of their responsibilities under the LEE Code of Conduct to behave honestly and with integrity and not make improper use of their position in order to gain, or seek to gain, a benefit or advantage for themselves or for any other person;

b. a letter of offer from Home Affairs, in 2018 indicating that they had read the LEE Terms and Conditions of Employment at the Phnom Penh Post. These terms and conditions:

i. outlined expectations that Officer K would abide by the LEE Code of Conduct as a condition of their employment;

ii. set out the grounds for termination of their employment; and

iii. defined 'serious misconduct' to include refusal to comply with the terms of the employment contract and divulging professional confidentiality;

c. a PDA in 2018 outlining their behaviours and responsibilities as an Enforcement and Engagement Officer which are referred to in paragraph 35;

d. a Direction from the Ambassador form from 2016 stating that they had read and understood the document which required LEE's to declare any conflicts of interest. Failure to do so may amount to a breach of the LEE Code of Conduct and the terms and conditions of their employment;

e. an acknowledgment of receipt of LEE Code of Conduct form from 2008 stating that they had read, understood and agreed to abide by the Code of Conduct for LEE's of the Phnom Penh Post; and

f. a Declaration of Secrecy form from 2008 stating that they would not reveal any information which came to their knowledge in the course of their employment or the discharge of their duties during the period of their employment or anytime thereafter unless authorised.

Conflict of interest

41. The LEE Code of Conduct required Officer K to disclose any real or perceived conflicts of interest related to their employment. A real conflict of interest occurs where there is a conflict between the public duty and personal interests of a LEE that improperly influences the performance of their duties. A perceived conflict of interest occurs where it appears that a LEE's personal interests could improperly influence the performance of their duties. If LEE's have contact with individuals such as former LEEs or migration agents, the contact is required to be declared to Phnom Penh Post as it could or could be seen to influence the LEE's in carrying out their official duties impartially.

42. Departmental records confirm that Officer K declared 25 conflicts of interest[13] during their time as a LEE. The most recent declarations were made on 9 and 15 January 2019.

43. Significantly, on 6 June 2011, Officer K declared contact with former LEE, Officer V, after meeting them briefly in a restaurant and receiving a phone call from them following their resignation to say goodbye. There were no documents recording further declarations made by Officer K regarding contact with Officer V following this declaration.

Interview with Officer K

44. During the course of the investigation, ACLEI investigators identified 20 allegations that amounted to possible breaches of the LEE Code of Conduct by Officer K.

45. ACLEI investigators travelled to the Australian Embassy in Cambodia to put these allegations to Officer K. The interview was held on 21 March 2019 and was conducted on a voluntarily basis.

46. The allegations put to Officer K can be grouped into four categories:

a. multiple inappropriate accesses to Home Affairs visa records relating to them and their immediate family members;

b. multiple inappropriate accesses to Home Affairs visa records, including at the request of unauthorised parties;

c. release of official information from Home Affairs records without appropriate authorisation; and

[13] Officer K submitted conflict of interest declarations to the department on 28 February 2011, 6 June 2011, 28 June 2011, 8 December 2011, 21 December 2011, 16 January 2012, 16 May 2012 (two declarations made on this day), 5 March 2013, 18 June 2013, 24 June 2013, 21 October 2013, 10 April 2014, 27 October 2014, 14 June 2016, 22 June 2016, 26 May 2017, 14 June 2017, 19 June 2017, 17 March 2017, 22 June 2017, 17 October 2017, 20 March 2018, 9 January 2019 and 15 January 2019.

d. failure to declare all real or perceived conflicts of interest that directly relate to their role at the Australian Embassy, Cambodia.

47. The four categories are expanded below.

Category 1: Access to records relating to Officer K and their immediate family members

48. Assessment of audit data contained in the Integrated Client Services Environment (ICSE)[14] identified that Officer K accessed data related to them 72 times from 6 January 2010 to 11 October 2018. Between January 2010 and February 2010, Officer K accessed their personal records 24 times. Of these 24 accesses, 12 related to the record of Officer K's refused VF 476 Skilled-Recognised Graduate application. This included access on 10 February 2010, which was the date this application was refused.

49. Assessment of audit data contained in the ICSE Offspring system indicated that Officer K accessed two of their own tourist visa applications in 2011 and 2012.

50. In addition to their own records, ICSE audit data revealed that Officer K accessed data relating to:

    a. their sibling, a total of 708 times from 22 February 2011 to October 2018;

    b. their partner, a total of nine times between 24 March 2010 and 11 October 2018;

    c. their in-law, eight times between 5 February 2014 and 12 November 2015;

    d. their mother, three times on 23 May 2017; and

    e. their father, two times on 23 May 2017.

51. During the course of the investigation, investigators analysed the accesses to their family member's records and established that:

    a. there were no records to indicate the accesses to Officer K's family records were authorised or for a 'business need';

    b. access to Officer K's own records and records of their family members would not be authorised under any circumstances; and

    c. there were no records to suggest Officer K had declared or explained their accesses.

52. In the first half of Officer K's interview on 21 March 2019, Officer K described to investigators what constituted the appropriate use of Home Affairs systems. Officer K explained they were not authorised to check on someone using Home Affairs systems just because they had an interest in them and gave an example of famous people. They further explained that they were only authorised to access Home Affairs' systems for information that related to their assigned work which was on a 'need-to-know' basis. Officer K explained that they were the only person who knew their password to the ICSE and ICSE Offspring systems.

53. When the allegations relating to Officer K's self-accesses were put during the second half of their interview, Officer K stated:

    a. they had accessed their own visa application;

[14] ICSE was one of the main visa processing systems used by Home Affairs at the time of the investigation.

b. the main reason for accessing their visa application was to find out what requirements of their visa application they had failed to meet so they could strengthen any future application;

c. they continued to view their application to stay up to date on what the requirements were for this skilled visa class; and

d. they did not have a business need to access their own records.

54. When the allegations relating to accesses to Officer K's family members were put to them, Officer K admitted they accessed the records of their family members and provided the following response:

a. They accessed their partner's records because they wanted to move to Australia to benefit their family's future. Officer K knew accessing their records and those of their partner's was against the LEE Code of Conduct;

b. Their family were concerned about Officer K's sibling living alone in Australia. As a result, Officer K first accessed their sibling's records when their sibling changed universities as Officer K was concerned their sibling would be issued with a non-compliance notice for not attending university. Further, Officer K stated that their sibling applied for a permanent visa in 2013 based on their relationship with someone they had met in Australia and Officer K viewed the visa application to understand its status. Officer K then acknowledged that access to their siblings records was not appropriate and was a conflict of interest;

c. Prior to their in-law marrying their sibling, Officer K wanted to learn more about them through the use of ICSE including their migration status and whether they had been married before. Officer K acknowledged that they were only able to obtain this information about their in-law by using their position with the Australian Embassy and that these accesses were not appropriate. Officer K stated that they did not provide any information to their in-law about their records as they were not friends;

d. They accessed their parent's records to obtain detailed information that would help their future visa applications. Officer K stated that no one asked them to look their parents up and acknowledged that this access was not appropriate; and they were aware of the policies surrounding access to people's record who were personally known to them; and

e. They did not access their family's records for the purpose of receiving any benefit or favour.

Category 2: Accesses to records without authorisation, including at the request of unauthorised parties

55. The investigation identified the following 2,748 accesses in relation to 7 visa applicants were in circumstances where Officer K did not have any official involvement in the applications and the accesses were not consistent with their duties:

a. audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person A 680 times between 28 June 2016 and 17 November 2016. When this allegation was put to Officer K during their interview, Officer K stated they probably checked this application on behalf of someone they knew in the community but did not state who they thought this person may have been. Officer K stated they would check the ICSE notes on a regular basis to monitor the progress of the application and see if the case officer needed any further documents or information. Officer K stated they had probably given feedback on the application's progress to the applicant or the applicant's family including whether more documents would be required. Officer K agreed that they did not have any official involvement in the processing of Person A's application.

b. audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person B 709 times between 2 December 2015 and 2 November 2016. When this allegation was put to Officer K during their interview, Officer K acknowledged they had no business need to access Person B's records. Officer K stated they were asked to check Person B's application by a family friend of their mother or father. They had been told that Person B had been waiting a long time and was desperate to migrate to Australia. Officer K stated they decided to monitor it so they could give feedback to Person B and let them know if there was further evidence that should be submitted.

c. audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person C 965 times between 23 January 2015 and 11 November 2016. When this allegation was put to Officer K during the interview, Officer K was not able to provide any explanation, business related or otherwise, as to why they had looked at Person C's records.

d. audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person D 142 times between 17 August 2017 and 7 September 2018. When this allegation was put to Officer K during their interview, they stated Person D may have been a relative of Officer V and believed Officer V had called Officer K about the application. Officer K then stated that Officer V would always tell them a family member needed migration assistance and that was why Officer K would agree to help. Officer K stated they would have only checked the application details or made sure it had been lodged.

e. audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person E 36 times between 12 March 2018 and 22 January 2019 (noting the audit was run on 23 January 2019). The application was still in progress during the investigation. When this allegation was put to Officer K during their interview, Officer K was unable to recall their reason for accessing Person E's records at first. Officer K believed it was possible that Officer V had also asked them about this application. Officer K then stated that they thought Person E was related to Person C given the sponsor of the application also had the same surname as Person C. Officer K then stated that the sponsor or Person E could be related somehow to Officer V.

f. audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person F 213 times between 10 May 2016 and 23 November 2016. When this allegation was put to Officer K during their interview, they stated they thought they viewed this application on behalf of a colleague of Officer K's mother and that Person F was either the daughter or niece of this person.

g. audit data of Home Affairs systems identified that Officer K had accessed the ICSE records of Person G three times between 1 July 2016 and 24 April 2017. When this allegation was put to Officer K during their interview, they agreed that they had no genuine business reason to access Person G's records.

Category 3: release of official information without appropriate authorisation

56. The investigation identified Officer K had disclosed official information without authorisation in relation to six visa applications which were referred to in photographed text messages on the located phone. Those applications are as follows:

Person H

57. A photo of the located phone identified a text message, sent on 27 June 2016 at 9:26pm Phnom Penh time containing a passport number.

58. The Home Affairs system identified this passport number was used by Person H.

59. Audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person H 73 times between 4 July 2016 and 29 May 2017.

60. In the first half of their interview, Officer K told investigators that they knew exchanging information or discussing a visa application with unauthorised persons could get them 'into trouble'.

61. When photographs of the phone's location and some of its content were presented to Officer K in interview, they acknowledged that they used this phone but claimed that it was their mother's phone and was mostly used by their mother.

62. When the allegations relating to Person H were put to Officer K, they stated:

    a. they accessed Person H's application after receiving the text message;

    b. their access was only for the purpose of checking the progress of the application and to determine if the applicant had submitted enough documents or if they were required to submit additional material;

    c. it was a friend or work colleague of their mother's who had requested to know the status of Person H's application. Officer K then reiterated it was their mother who used the phone and people messaged their mother requesting status updates in relation to their visas. Officer K claimed that if they were not seen to assist people in their community, it would lead to people being jealous of or thinking 'bad things' about their family;

    d. they received a benefit in terms of reputation and status within the Cambodian community by providing this information to their mother or their mother's associates; and

    e. Person I had sent Person H's passport number to the located phone. Officer K claimed that they were no longer in contact with Person I but had been in contact with them throughout 2016 and 2017.

Person J

63. A photo of the located phone identified that the text message which contained the passport number of Person H also contained passport number belonging to Person J.

64. Audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person J 201 times between 1 July 2016 and 20 November 2017.

65. When this allegation was put to Officer K during their interview, they stated:

    a. they had no business reason to access Person J's records in ICSE and agreed that they were monitoring the application;

    b. Person J was probably related to Person I because Person J's spouse is the sibling of Person I.

c. they only checked the progress of the application and made sure enough documents had been provided. They did this because Person I wanted to know the progress of the application and wanted to know if more documents or information could be submitted to speed up the processing. They told Person I they would update them on the status of the application; and

d. they knew the policy was to direct people who asked about the progress of visas to the Home Affairs website and other public contact details. Officer K further acknowledged when someone persistently asked them about visas they were obligated to report this contact.

Person L

66. Photos of the located phone identified a text message dated 22 September 2018 sent by the contact number associated with Officer V. The text message contained the full names and dates of birth for Person L and Person M. The details were accompanied by "*case already lodge please if good or not*". Also photographed was a reply message from the phone, sent two minutes after the text was received, which read "*…. Noted. Will do on Tuesday cos public holiday*".

67. ICSE records revealed Person L had applied for a prospective marriage visa application and Person M was listed within Person L's application as their sponsor.

68. Audit data of Home Affairs systems identified Officer K accessed the ICSE records of Person L 72 times between 25 September 2018 and 22 January 2019 (noting that Officer K's ICSE audit was run on 23 January 2019). These audits revealed Officer K first accessed Person L's records on the Tuesday following the date of the text message, being 25 September 2018.

69. On 9 January 2019, authenticity concerns were raised in regards to one of the documents provided in Person L's visa application. Procedures at Phnom Penh Post allow for case officers to verbally consult with Officer K, in their capacity as Engagement and Enforcement Officer, in order to verify the authenticity of documents. Access to Person L's records to undertake a verification check would have been considered part of Officer K's duties.

70. The investigation established that prior to 9 January 2019 and after completing the verification check on or around 9 January 2019, Officer K had no business requirement to access Person L's records. Officer K made 54 accesses to Person L's records before any concerns surrounding Person L's documents were recorded by any Home Affairs staff members. Further, there were no records to indicate that Officer K had, at any time, declared they had been in contact with this applicant.

71. When this allegation was put to Officer K during their interview, they stated:

a. they had first accessed this application at the request of Officer V;

b. Officer V asked them to check the progress of Person L's application as Person L was a family member of Officer V;

c. after receiving the text message from Officer V, they accessed Person L's records in ICSE to see where the application was up to;

d. they had continued to monitor the status of this application; and

e. that what they were doing was the 'wrong thing' to do.

Other disclosures relating to Category 2

72. During the interview with Officer K about their unauthorised accesses to visa records referred to in **Category 2**, it was determined that Officer K had also disclosed official information in relation to the following visa applications without authorisation:

    a. Person D – The decision maker in Person D's visa application identified that there was a need to undertake an interview with Person D due to an allegation that Person D was in a contrived marriage for the purpose of obtaining a visa. Officer K advised they were unaware of any plans to create a fake or contrived relationship for Person D, however they told Officer V about the allegation involving Person D. Officer K was asked if Officer V offered them anything in return for checking Person D's records. Officer K stated that there was no offer of money as it complicated the situation and caused reputational issues. Similar to earlier statements, Officer K said they did it in exchange for having a good future relationship and friendship with Officer V. Officer K pointed out that they, their spouse and other close family members all had very good jobs and they did not need any extra money.

    b. Person E - Officer K stated that Officer V would have only wanted an update on the progress of the application. Officer K was asked if Officer V offered them anything for checking Person E's records, to which Officer K stated they had not. Officer K stated that Officer V would have only wanted to know which part of the visa process the application was up to.

    c. Person F - Officer K stated they accessed Person F's records on behalf of a colleague of Officer K's mother and that Person F was a relative of this person. Officer K advised they provided feedback on where the application was up to and that was all they could do. Officer K said they felt 'annoyed' that they continuously asked their mother about the progress of the application.

Category 4: Failure to declare all real or perceived conflicts of interest that directly relate to their role

Person I

73. Investigators observed several text messages in the located phone that suggested Person I had been in contact with the located phone regarding several visa applications in 2014 and 2016. There were no records to suggest Officer K had declared a conflict of interest in relation to their involvement in or access to Australian visa applications associated with Person I. There were no records to suggest Officer K advised Home Affairs of any inappropriate contact by Person I.

74. One of the messages on the located phone was sent on 3 November 2014 and contained the full name of the sibling and niece of Person I. The message containing these details finished with the phrase "*really appreciates your help*".

75. Case notes on the file of Person I's sibling's file identified Officer K was involved in processing the siblings' visa application on the day it was granted, being 4 December 2014. According to these notes, Officer K responded to an email from Person I's sibling after they requested a status update on the visa applications belonging to themselves and their child. There were no records contained in these case notes or on Officer K's personnel file that they had declared any potential conflict of interest in regard to either of these applications despite them apparently being contacted by Person I on the located phone about the two applicants just over a month prior.

76. When the allegation was put to Officer K about failing to declare contact with Person I, they stated:

    a. they had declared their association with Person I to a former PMO at Phnom Penh Post in 2011 but they could not recall how they declared this association; and

    b. they did not declare being approached about the visa application of Person I's sibling in 2014, even after they had official involvement in processing the application.

Officer V

77. Text messages on the located phone showed contact with the number associated with Officer V as far back as 2014 and as recently as September 2018. Further, the located phone showed 298 missed calls from Officer V's phone number.

78. A review of all the captured text messages between the located phone and the contact number for Officer V indicated the messages appeared to relate to the transfer of money and the request for information in relation to specific active visa applications.

79. The investigation established that Officer K had made no further declarations regarding contact with Officer V since their declaration on 6 June 2011.

80. In the first half of the interview, Officer K was asked whether they had any contact with Officer V since their resignation in 2010. Officer K stated they had breakfast once or twice in the same restaurant as Officer V 'a long time ago' but they had only briefly said hello to each other. Officer K stated they never spoke to Officer V about the circumstances of their resignation but Officer K felt nervous interacting with them because the resignation was "unusual" in the sense that it was sudden and unexpected. As such, Officer K stated they did not want to get "involved" with Officer V. Officer K claimed they had not had any further contact with Officer V since the brief encounter at the restaurant.

81. Officer K further explained they knew Officer V when they both worked together at Phnom Penh Post but Officer K did not know them very well as they were only work colleagues. Officer K stated they did not work on any visas for persons associated with Officer V.

82. During the second half of the interview, Officer K explained they did not tell investigators about their contact with Officer V in the first half of the interview because they knew that Officer V had some previous issues with Home Affairs and they believed this would therefore affect them. It was for this reason that Officer K also did not declare their contact with Officer V to Phnom Penh Post.

83. When the text messages contained in the located phone were put to Officer K, they stated:

    a. they did not declare any of their phone contact with Officer V, including when Officer V had asked Officer K to help with Australian visas;

    b. they were aware of their obligations to declare their contact with Officer V;

    c. they would classify their friendship with Officer V as 'good friends' and they did not want to cut off contact with Officer V; and

    d. Officer V was only in contact with them on an occasional basis.

84. Photographs obtained of text messages within the located phone under Officer K's workstation identified contact with Officer V's contact number which appeared to relate to the payment of funds to the user of the phone, including:

a. Officer V messaging the phone on 24 November 2014 with "*Money is ready I think we should meet in front of...*" (note: the rest of this message was not captured in the sample taken from this phone);

b. A message from the phone to Officer V dated 11 May 2018 which read "*i got all $. Thanks...* "; and

c. Another message from the phone to Officer V dated 29 June 2018 which read "*Thanks ... Is this wing?*"

85. When the text messages regarding payment of funds were put to Officer K, they stated:

a. the messages "have something to do" with their mother;

b. the messages relate to a loan Officer K's mother had given Officer V and Officer V was trying to return it;

c. "wing" is a reference to Cambodia's mobile money transfer platform "Wing Money Transfer & Payment Services"; and

d. the repayments were made in small instalments over the years and some of these were made using the Wing Money Transfer & Payment Services.

86. When explaining the $10,000 USD loan to Officer V, Officer K stated that:

a. in 2014 Officer V urgently needed money. As a result of this, Officer V asked to borrow money from Officer K and Officer K's mother. Officer K did not have money to loan however Officer K's mother loaned Officer V about $10,000 USD;

b. Officer V contacted other people to borrow money because they needed more than $10,000 USD;

c. they do not know how much is left to repay on the loan owing to their mother, but they thought it might be "a few thousand";

d. Officer K's mother, was from the "old generation" in Cambodia who did not keep her money in a bank account;

e. Officer V paid Officer K's mother interest on the loan; and

f. there was no contract between Officer V and Officer K's mother for the loan because the two parties trusted each other.

87. Officer K stated that the payments received from Officer V were not in return for disclosing information about visa applicants. At various times in the interview, Officer K was asked what benefit they received from Officer V for assisting with the visa applications. Officer K advised:

a. that Officer V had a relative in Australia and that should Officer K visit Australia again, they could stay at their residence; and

b. Officer V was in a 'good family' and had a 'good' business. Officer K said they knew Officer V had business contacts that may be able to help them in the future, potentially with other job opportunities.

Allegations involving the imposter immigration email address

88. On 1 November 2018, the PMO within Phnom Penh Post reported an integrity incident that had occurred the previous day to both I&PS and ACLEI.

89. The report stemmed from a call to Phnom Penh Post by visa applicant, Person M, the day before. Person M contacted Phnom Penh Post to advise they could not attend an interview scheduled for that day, however staff at Phnom Penh Post were unable to

locate the appointment. After conducting system checks and confirming no appointment had been scheduled for Person M, the following information from them:

a. Person M had been receiving emails about their interview from a Gmail email address which they were able to provide to the department;

b. Person M had not met anybody at Phnom Penh Post or outside of the embassy grounds to discuss their application;

c. Person M had not paid money to anyone; and

d. the sponsor of Person M's application received a phone call from "Immigration in Australia", informing them of the scheduled interview.

90. On 31 October 2018, Person M emailed the first name, contact number and the DFAT email address of the person who had contacted them about their visa application.

91. The investigation established:

a. No DFAT email accounts were found to be in contact with the Gmail address provided by Person M;

b. The contact number was registered to the DFAT Melbourne office but not to a particular employee;

c. No user existed with the email address provided by Person M; and

d. No records in the incident report indicating that anyone from the Phnom Penh Post would have been calling the sponsor of Person M's application.

92. As such, it is unknown who in DFAT was calling the sponsor.

93. During the investigation, systems audits were undertaken to ascertain which staff members at Phnom Penh Post had accessed Person M's or their sponsor's visa applications. The audit identified visa processing officer, Officer Z, accessed the sponsors ICSE records once on 11 October 2018, without an apparent business need. It was further discovered that Officer Z may have accessed a total of six other visa applications without a business need.

Officer Z

94. Officer Z commenced employment as a LEE with Phnom Penh Post around mid-2012. From 2015, Officer Z was a visa processing officer.

95. The investigation obtained training records which confirmed that Officer Z had completed 196 training modules between 3 July 2012 to 6 March 2019. A significant portion of this training related to fraud and corruption awareness as well as conduct and behaviour.

System audits relating to Officer Z

96. Following the identification of Officer Z, on 1 February 2019 ACLEI obtained a full ICSE access audit for Officer Z from the date they commenced employment with Phnom Penh Post.

97. On 25 March 2019, a number of email enquiries were located which sequentially followed the access by Officer Z on 11 October 2018. The investigation determined it was plausible that Officer Z had accessed these applications to see if the related enquiries were associated with their caseload. As such, the investigation focused on the six accesses identified from the full ICSE audit.

Evidence obtained during the investigation

98. Whilst in Cambodia, Officer Z was invited to an interview with ACLEI in relation to the allegations. Officer Z agreed to speak to the investigators and the interview was held on 26 March 2019 at the Australian Embassy. The six allegations put to Officer Z in interview are outlined below:

Allegation 1: Person N

99. Assessment of audit data contained in ICSE identified that Officer Z accessed records related to Person N 14 times from 27 September 2018 to 22 February 2019 without a known business need.

100. Further, audit data revealed that Officer Z accessed the records of a different person with the same name as Person N eight times on 26 October 2018 and 3 January 2019, without a business need.

101. Prior to any allegations being put to them, Officer Z stated that they liked 'researching' and being 'curious' in their work. Officer Z explained this meant they asked their supervisors a lot of questions to the point where they felt they were beginning to annoy them. Officer Z stated this led them to conduct further research in order to answer their own questions where possible.

102. When the allegation was put to Officer Z, they stated that they wanted to learn from other applications so they could contribute to their team to make sure their applications were of the same standard and followed consistent workflows.

103. It was put to Officer Z that they were trying to find an application and to pass information outside of Phnom Penh Post. In response to this, Officer Z stated that:

    a. they knew visa officers could be offered money to provide confidential information but they respected their values and their workplace so they would have no reason to engage in such activity;

    b. no one asked them to look up this application;

    c. they would not sell their values or the respect they had for their workplace, particularly when they had worked at Phnom Penh Post for so long and had studied hard in order to get a good job; and

    d. from their perspective, they did not have any intention to provide the visa applicant's information to anyone.

Allegation 2: Person O

104. Assessment of audit data revealed that Officer Z accessed records related to Person O 20 times from 10 October 2017 to 5 March 2019 without a known business need. Person O was involved in an application to the Administrative Appeals Tribunal (AAT) after their prospective marriage visa was refused.

105. When investigators put this allegation to Officer Z, they stated:

    a. they accessed the records only because they were curious to learn about complex applications to the AAT;

    b. they did not have any other purpose than just wanting to learn and improve the quality of their work;

    c. they had been told by their MCO that they may be asked to grant permanent class visas, not just assess them, and this motivated Officer Z to learn more about permanent visa processing;

d. sometimes they became bored with the caseload they were working on so would sometimes view applications handled by their colleagues so they could read and learn about something new or different;

e. they had no ulterior purpose for accessing applications assigned to their colleagues other than to learn from them;

f. they did not access these applications in return for money or favours; and

g. nobody asked them to look up Person O's applications.

Allegation 3: Person P

106. Assessment of audit data revealed that Officer Z accessed records related to Person P 43 times from 5 July 2018 to 15 January 2019 without a business need.

107. The assessment also revealed that Officer Z accessed records related to Person P's spouse and child a total of 13 times between 5 July 2018 and 22 October 2018, without a known business need.

108. When this allegation was put to Officer Z during their interview, they stated that:

a. the applicant had changed their visa class and this was something new to Officer Z. As a result, Officer Z wanted to learn about the application;

b. nobody asked Officer Z to check Person P's application; and

c. if somebody asked Officer Z to check the status of Person P's application, they would have reported it as it is against the LEE Code of Conduct.

Allegation 4: Person Q

109. Assessment of audit data revealed Officer Z accessed records related to Person Q 48 times from 19 April 2018 to 22 February 2019 without a known business need.

110. When this allegation was put to Officer Z, they stated:

a. there were not many complex applications for Australian based applications but there were in the offshore cohort and that Person P's application was one of these complex applications; and

b. they overheard their colleagues discussing the application and wanted to look into it to learn from it; and

c. nobody asked them to look it up.

Allegation 5: Person R

111. Assessment of audit data revealed Officer Z accessed records relating to Person R five times on 17 December 2018, without a business need. Further, the data revealed that Officer Z also accessed the records of Person R's father, eight times on 17 December 2018 without a known business need.

112. When this allegation was put to Officer Z, they stated that:

a. they did not remember why they had accessed these records;

b. they may have viewed the application because they were 'curious' but they cannot recall the applicant's name;

c. nobody from outside Phnom Penh Post asked the, to look at the records and stated that if this happened they would have reported it to their manager.

Allegation 6: Officer U

113. Assessment of audit data revealed that Officer Z accessed records relating to former work colleague, Officer U four times on 11 December 2018, without a known business need. Further, the data revealed Officer Z also accessed records related to Officer U's partner three times on 11 December 2018, without a known business reason.

114. The investigation did not locate any documents to indicate Officer Z declared accessing the records of their former colleague.

115. When these allegations were put to Officer Z during the interview, they stated that:

    a. they had come across Officer U's ICSE records by accident when looking for someone with a similar name and wondered whether the records were their former colleagues. As such, Officer Z opened the records and viewed the photo to confirm whether it was Officer U;

    b. Officer U had told Officer Z and other LEEs that they were travelling to Australia to look after a sick relative but Officer Z overheard another colleague discussing Officer U's plans in Australia which were different to what Officer U had told Officer Z. Officer Z believed they had been lied to by Officer U so they looked into Officer U's application to confirm the reason they travelled to Australia;

    c. their colleague would talk to Officer Z occasionally about Officer U and their time in Australia which made Officer Z "more curious" about what Officer U was doing;

    d. they knew they should not have looked into Officer U's record but they did not pass the information they obtained from accessing these records on to anyone;

    e. they did not declare the access because they did not want to cause suspicion; and

    f. they were not very friendly with Officer U.

Findings

116. I am required under s 54 of the LEIC Act to provide my findings on the corruption issues.

117. I am satisfied that the evidence obtained in the course of Operation Chandra that Officer K and Officer Z engaged in corrupt conduct, namely, abuse of office and corruption of any other kind.[15]

118. 'Abuse of office' is not defined in the LEIC Act. It is a concept primarily used in the context of criminal law. It generally involves using one's office, or the information obtained in their official capacity, to dishonestly benefit oneself or another, or to dishonestly cause detriment to another.[16]

119. 'Corruption of any other kind' is also not defined in the LEIC Act. It generally involves a staff member engaging in conduct which was

[15] Law Enforcement Integrity Commissioner Act 2006 (Cth), ss 6(1)(a) and (c)

[16] Criminal Code (Cth), s 142.2(1).

a. a deliberate act of dishonesty, breach of the law, or abuse of public trust or power that undermines or is incompatible with the impartial exercise of an official's powers, authorities, duties or functions; or

b. a moral impropriety in, or in relation to, public administration.[17]

120. While my findings concern corruption, not criminality, I consider these general elements expounded in the criminal law useful in considering whether a staff member of a law enforcement agency has engaged in conduct involving an abuse of their office.

121. As a LEE, Officer K and Officer Z were obliged to adhere to the standards of behaviour specified in the LEE Code of Conduct. In particular, they were required to:

a. behave in a way that upholds the integrity and good reputation of Phnom Penh Post;

b. behave honestly and with integrity in the course of their employment with Phnom Penh Post;

c. not use their official position to influence improperly or try to influence colleagues or members of the public by giving or receiving gifts or by entering into financial or other arrangements with them;

d. maintain appropriate confidentiality including about information obtained during the course of their employment;

e. not misuse information obtained in the course of their duties or disclose it to any person unless they were authorised to do so;

f. disclose and take reasonable steps to avoid, any conflict of interest, either real or apparent, in connection with their employment in the Phnom Penh Post;

g. disclose any interests, financial or otherwise, including in respect of family and friends, that could conflict with the proper performance of their duties. They must also take whatever action is necessary to avoid that conflict; and

h. not make improper use of inside information, or their duties, status, power or authority in order to gain, or seek to gain, a benefit or advantage for themselves, or for any other person. This extends to their family, where the gift or benefit is a direct result of their official duties.

122. The LEE Code of Conduct specified that Officer K and Officer Z were required to adhere to Australian principles and standards of conduct in the workplace. The core underlying principles of such conduct, include:

a. to act in accordance with local law and applicable Australian law;

b. to deal equitably, honestly and in a professional manner with both the public and colleagues;

c. to ensure there is no real or apparent conflict of interest; and

---

[17] Independent Commission Against Corruption v Cunneen (2015) 256 CLR 1 at [76].

d. to ensure their professional or personal behaviour does not bring the Australian Embassy or the Australian Government into disrepute.

Findings in relation to Officer K

123. On the basis of the evidence and material collected and analysed in the course of Operation Chandra I find the following:

a. Officer K accessed their own visa records to review the basis on which their visa application was refused by Home Affairs and to use this information to benefit their future applications in a way that an ordinary member of the community would not be able to do.

b. Officer K deliberately accessed records in the Home Affairs systems related to their family members and members of the Cambodian community without a business need. Furthermore, the seriousness of Officer K's conduct is compounded by the use of the Home Affairs systems to:

   i. covertly conduct a 'background check' on their potential in-law to ascertain whether they were of good character and had been married before; and

   ii. monitor their sibling's attendance at university in Australia.

c. The disclosure of visa information to Person H, Person J, Person L, Person E and Person F (referred to in Category 3), meant they had access to visa information they may not have been privy to had it not been for their association with Officer K. It also allowed these applicants to circumnavigate the processing timeframes within Home Affairs and enabled them to receive visa information quicker than they otherwise would have.

d. Officer K failed to declare conflicts of interest following their contact with Officer V, Person I and visa applicants whom they were in contact with on the located phone. The declaration of actual, potential or perceived conflicts of interest is a key mechanism used by public sector agencies to identify the risks facing staff members and their ability to effectively and impartially perform their duties. Disclosing associations with these people would have enabled Phnom Penh Post to manage these risks by, for example, adjusting Officer K's duties or requiring them to remove themselves from the conflict. Given the concealed nature of their contact with these people on the located phone, I am satisfied that Officer K did not declare their association due to their awareness of the consequences that would follow having such relationships.

e. I am not satisfied there is sufficient evidence to conclude that Officer K received a financial benefit through accessing and disclosing information. However, I find that Officer K received a personal benefit for assisting Officer V. Officer K stated during interview that they completed these checks for Officer V in order to maintain a good relationship for Officer K to leverage off in the future.

f. In addition to a personal benefit, I am further satisfied that Officer K's conduct was motivated by obtaining an intangible benefit, known as 'social capital'. Social capital is the non-monetary benefit or improved social standing that can be gained through engaging in corrupt conduct. Officer K undertook unauthorised checks and disclosed official information in order to increase the standing and reputation of their family within the local Cambodian community. Even by their own admission, Officer K acknowledged that if they were not seen to assist people in their community, it could lead to reputation damage for their family.

g. The gravity of Officer K's conduct is exacerbated by their position as Enforcement and Engagement Officer at Phnom Penh Post. Officer K's position required them to operate under Home Affairs' integrity framework on a daily basis by, amongst other things, conducting integrity checks and identifying integrity issues within visa processes. As such, I am satisfied that they held an intricate understanding of the policies and laws around appropriate use and disclosure of official information and the need to declare all real or perceived conflicts of interest.

124. Accordingly, I find that pursuant to ss 6(1)(a) and (c), Officer K engaged in corrupt conduct.

Findings in relation to Officer Z

125. On the basis of the evidence and material collected and analysed in the course of Operation Chandra I make the following findings:

Access to records relating to former colleague, Officer U

126. The investigation did not identify any evidence that Officer Z had authorisation or an official business need to access the records of their former colleague, Officer U. The investigation did uncover records that showed Officer U's visa application was transferred to a different office for processing in order to minimise the possibility of Officer U's work colleagues having any official involvement in their application. Furthermore, the investigation did not locate any records to suggest Officer Z had previously come forward and declared their access to Officer U's records, as is the usual procedure when an employee accesses a record related to someone they know personally.

127. Officer Z's conduct was in breach of their responsibilities under the LEE Code of Conduct. Specifically:

- *An employee must use the resources of the Australian Embassy, Phnom Penh in a proper manner.*

  ……..

- *The property of the Australian Embassy is to be used for official purpose only, and is to be used efficiently and effectively.*

128. I am satisfied that Officer Z understood what constituted appropriate and inappropriate access to Home Affairs information. By their own admission, Officer Z told investigators that their actions in accessing Officer U's records were "wrong" and that it was against Home Affairs policy to do so. Officer Z's integrity training records indicated they were aware of Home Affairs policies regarding inappropriate access to systems.

129. Importantly, had it not been for Officer Z's position as a staff member of Home Affairs, they would not have been privy to the visa information relating to Officer U.

130. Accordingly, I am satisfied that in engaging in the aforementioned conduct, Officer Z engaged in corruption of any other kind pursuant to s 6(1)(c) of the LEIC Act. Officer Z deliberately, and in contravention of their obligations under the LEE Code of Conduct, accessed the information of their former colleague to satisfy their curiosity. It was an inappropriate use of Commonwealth resources.

Accesses relating to remaining five visa applicants - Person N, Person O, Person P, Person Q and Person R

131. While the evidence obtained in the course of Operation Chandra supports a conclusion that Officer Z engaged in improper conduct in relation to the remaining six accesses, I am not satisfied that these accesses support a corruption finding.

132. The evidence demonstrates that Officer Z breached policy by accessing visa records which were allocated to their colleagues. Officer Z's explanation throughout the interview was mostly consistent. They assert that they accessed the records in order to learn more about visa processing to inform their work.

133. The investigation found that Officer Z likely perceived the accesses to be work-related. The investigation did not find any evidence which contradicted Officer Z's statements that they had not released official Home Affairs information without authorisation, or that they had misused the information by attempting to influence the processing of visas.

134. It is clear that Officer Z breached policy and duties by accessing these five visa applicants. However, I am not satisfied that the evidence demonstrates that they engaged in corrupt conduct in doing so.

Action under Part 10 of the LEIC Act

135. On 19 June 2019, LEE Code Investigation and Determination reports regarding the investigations into Officer K and Officer Z were completed and provided to DFAT.

Corruption Prevention Observations

136. This investigation formed part of ACLEI's Visa Integrity Taskforce (VITF). The VITF was established in 2017 by the then Integrity Commissioner to target corrupt conduct by staff members involved in the processing of visas in various Australian overseas posts. The Taskforce officially concluded on 30 June 2020, although some related investigations are still being finalised. Whilst the VITF has concluded, this investigation highlights corruption risks and vulnerabilities along with risk mitigation strategies which have since been implemented.

137. At the time of the corrupt conduct, Home Affairs had, in cooperation with DFAT, implemented an integrity framework for visa processing at Australian overseas posts. These included a dedicated integrity unit at post; mandatory acknowledgments of and undertakings to comply with the LEE Code of Conduct; declarations of private, financial and other interests and secrecy; and mandatory training inclusive of online courses relating to integrity and visa processing. Despite these risk mitigation measures, the corrupt conduct occurred due to systemic and cultural vulnerabilities.

138. This investigation highlights the significance that social capital can have as a motivating factor for corrupt conduct, to the extent that it can be perceived by the employee to override their official responsibilities. Officer K repeatedly stated that they knew they were not authorised to access and disclose the information identified in this report, and also confirmed they were aware of the associated conflicts of

interest. Ultimately, however, they were more motivated by their desire to retain and potentially elevate their social standing in the local community.

139. Social capital was also intentionally leveraged by Officer V in the form of reach back. Reach back occurs when former employees seek out serving employees, who may feel pressured to provide favours, access or information due to a sense of misplaced loyalty, or the repayment of a debt or favour.[18]

140. To effectively mitigate against the risks associated with social capital and reach back, agencies must ensure they identify, assess and treat the unique risks within their operational environment[19]. Examples of controls that can be effective in reducing these risks can include:

    a. Effective management oversight and training. Front-line managers are in a unique position to understand the social context and pressures faced by their team. Effective training for managers can equip them to support their staff and drive high performance, or address / escalate any performance or integrity concerns.[20] Performance management programs can also be used to hold managers accountable for monitoring and responding to integrity risks.

    b. Fit-for-purpose systems access controls that include proactive monitoring. These could have enabled early identification of the ongoing unauthorised access engaged in by Officer Z and intervention to avoid the situation escalating; and

    c. Tailored integrity training that specifically addresses the risks of social capital and reach back, as well as what, when and how to report any requests for or examples of unauthorised access. Using real-life but anonymised examples can be an effective way to demonstrate the impact and consequences of corruption, and highlight that instead of improving an official's reputation, it is more likely to result in their social standing being significantly undermined.

141. ACLEI and Home Affairs officers involved in the VITF provided briefings and anti-corruption training to both Australian-based staff and LEEs in a number of overseas posts whilst on location. This training raised awareness of the integrity and corruption risks associated with visa processing and whilst highlighting the investigation capabilities of both agencies in relation to these matters, created a strong deterrent for future offenders. Senior officials were also briefed to tighten processes and procedures to ensure risks are managed appropriately at a local level.

142. ACLEI has published a range of fact sheets addressing different drivers of corruption, including social capital, grooming, reach-back, conflicts of interest, and the risks that these present.[21] These are available on the ACLEI website and were drawn to the attention of visa processing officers at Australian overseas posts following this investigation. ACLEI regularly presents to Home Affairs officers prior to their deployment on integrity risks, mitigation strategies and reporting requirements.

---

[18] ACLEI Corruption Prevention Concepts: Grooming (https://www.aclei.gov.au/sites/default/files/18362_-_aclei_-_corruption_prevention_final.pdf?acsf_files_redirect)

[19] ACLEI Corruption Prevention Concepts: Social Capital (https://www.aclei.gov.au/sites/default/files/aclei_factsheet_-_corruption_prevention_concepts_-_social_capital.pdf).

[20] ACLEI Corruption Prevention Concepts: Frontline Manager Capability (https://www.aclei.gov.au/sites/default/files/aclei_corruption_prevention_concepts_factsheet_-_frontline_management_capability.pdf)

[21] ACLEI website, Corruption Prevention Factsheets (https://www.aclei.gov.au/corruption-prevention/corruption-prevention-factsheets).

143. In response to this report, Home Affairs provided information on a number of initiatives that have been implemented to address the issues raised in this report. This information is set out in attachment A.

Jaala Hinchcliffe
Integrity Commissioner
23 December 2021

Attachments

Attachment A – Submission by Home Affairs

A number of developments and changes have occurred within Home Affairs since 2018-2019 that address issues observed during ACLEI's investigation and associated Visa Integrity Taskforce (VITF) investigations.

Some of these are broad reaching across the visa processing network, and some are more specific to the post that is the subject of Operation CHANDRA. There has also been action taken with respect to the two specific LEE identified in the report.

Broad reaching changes across the visa processing network

These are accurately outlined at paragraphs 149 (page 31) of the reports, and can be summarised as:

a. Updates to mandatory training to include specific fraud and corruption content. This builds staff capability to identify fraud, corruption and misconduct at overseas posts.

b. Visa and citizenship decisions are regularly reviewed by management as part of a strengthened quality management framework.

c. Updates to Home Affairs' systems that manage case allocation to allow greater control and audit capability by managers.

d. Implementation of a regular audit by overseas post managers of key integrity and other administrative controls to both identify and prevent fraud, corruption and misconduct.

e. Deployment of Caseload Risk and Integrity Teams in visa processing hubs to review and analyse caseload risk indicators

In addition, Home Affairs has implemented the following actions to address the issues of inappropriate access to systems (paragraph 149 b and c) and 'social capital' (paragraphs 147-148) raised in the report on Operation CHANDRA.

a. Since 2018, significant work has been undertaken within the Department to set the framework for providing a safe and secure environment for its people, information and assets, including developing the Protective Security Strategy 2025, Integrity Strategy 2025, and Cyber Resilience Strategy 2025.

b. The Department's Integrity Strategy 2025 includes an annual communications plan, training and awareness activities. Since the events in the report, the Department has published all staff messages promoting ACLEI videos and factsheets on grooming and unauthorised disclosure. Additionally, the Department has released informational videos and published a number of messages incorporating de-identified case studies to remind staff on their integrity obligations. Most recently (2021), the Department has rolled out specific offshore integrity scenarios and workshops to posts, which draw on real-life examples to highlight the consequences of misconduct and corruption.

c. Integrity and Professional Standards Branch continues to deliver preventative, detective and responsive controls in relation to integrity and corruption risks, in line with Integrity Strategy 2025. This includes early intervention strategies—for

example, by leveraging the Integrity Active Detection Program through the Unauthorised Access Campaign (which ran from 2 November to 31 December 2020) aimed at preventing and disrupting potential high-risk misconduct by users of certain systems.

d. Integrity risks—including conflict of interest and unauthorised access to systems—are identified within the Department's Enterprise Risks and addressed by the Department's Integrity and Professional Standards Frameworks and related policies.

Action taken with respect to the two locally engaged employees - Officer K and Officer Z

Both staff members with adverse findings under Operation Chandra are no longer employed by DFAT or the Department of Home Affairs.

Officer K's employment with Phnom Penh post was terminated in mid-2019.

Officer Z resigned in early 2020.

Specific actions taken with respect to Phnom Penh post

The current Principal Migration Officer (PMO) in Phnom Penh has confirmed that the following mitigation measures are in place which directly relate to the observations made in Operation Chandra. These are in addition to those measures identified for the entire visa processing network, and include:

Training and modelling

- LEE and A-based mandatory completion of fraud and corruption awareness training.
- A-based modelling of the APS Values and the Code of Conduct and explicit undertakings by LEEs in Performance Development Agreements (PDAs) to model this behaviour.
- Team participation in PMO-led integrity workshops and staff group discussions on integrity case studies within the context of Integrity Strategy 2025.
- PMO promotion and engagement of team on the Integrity toolkits.
- The establishment of a Phnom Penh visa integrity group drawing on the objectives of the Caseload Risk and Integrity Section in Immigration Programs Division.
- Adoption of an approach to general skilling of all officers in integrity related-work and the holding of team meetings to discuss integrity within the caseload.
- Pre-deployment training of A-based staff on the potential for corruption, Code of Conduct and reporting requirements.

Reporting obligations

- LEE complete annual Code of Conduct and conflict of interest declarations regarding interaction with persons that may form a perceived or actual conflict.
- LEE are required to report to the PMO any and all occasions they are approached regarding information on visas.
- PMO has emphasised LEE obligations with all staff at Phnom Penh post to remove pressure on Home Affairs' LEE.

- PMO has also advised Post employees on appropriate channels for information through the relevant website and Global Service Centre.
- Requirements placed in PDAs that specifically target the behaviours and vulnerabilities identified through Operation CHANDRA.
- Explicit undertakings by LEE regarding Code of Conduct and integrity and professionalism within PDAs and PDA discussions.
- Enforcement of PDA obligations to update declarable circumstances and real/perceived conflicts of interest and routine reminders on these obligations by the PMO.
- LEE subject to annual declarations regarding on-going contact with former staff, and immediate declarations regarding any actual conflict of interest or the potential for a perceived conflict of interest stemming from these relations.
- Explicit undertakings in PDAs regarding appropriate access to systems and information as per clearance and on a need to know work related basis and to report any actual or perceived breach.
- Explicit performance requirements in PDAs regarding obligations on reporting others where there is suspected misconduct or conflict.
- A-based staff required to refer allegations, suspected or potential breaches to IP&S and report to Overseas Immigration Coordination Section and DFAT.

Almost all staff have reported some recent form of contact with the persons of interest under Operation Chandra, which indicates that reporting requirements are known and being followed.