



Australian Government
Department of Immigration
and Border Protection



Australian
BORDER FORCE



Australian Government

Fair Work
OMBUDSMAN

TASKFORCE CADENA

JOINT AGENCY AGREEMENT

Foundation agreement for the formation of a taskforce for the conduct of multi-agency operations targeting visa fraud, illegal work and the exploitation of foreign workers

Department of Immigration and Border Protection

Australian Border Force

Fair Work Ombudsman

Released by DIBP under the
Freedom of Information Act 1982

Version 3.0

Purpose

1. The purpose of this Joint Agency Agreement (JAA) is to ensure that all parties involved in Taskforce Cadena have a clear understanding of the objectives and key deliverables of the Taskforce and the general principles governing its operation.

Parties

2. This Joint Agency Agreement (Agreement) is made between the following parties:
 - Department of Immigration and Border Protection (DIBP);
 - Australian Border Force (ABF); and
 - Fair Work Ombudsman (FWO)

Background

3. The incidence of fraud and exploitation involving foreign workers in Australia is well-known to DIBP and FWO. A range of integrity and investigative initiatives have been actively progressed across these agencies through ongoing campaigns, enquiries, investigations and field operations.
4. Targeting and disrupting entities which seek to commit visa fraud and exploit foreign workers is a priority of DIBP, FWO and other regulatory agencies.
5. Taskforce Cadena will initially focus on the collective information holdings of DIBP, FWO, the Australian Federal Police (AFP), and other agencies. Further action will be considered and linked to broader coordinated activity across government to address the matters related to illegal work and the exploitation of foreign workers.

Objectives

6. To reduce visa fraud, illegal work and the exploitation of foreign workers in Australia.
7. To utilise intelligence from a range of sources to identify and investigate major targets of interest.
8. To influence Australian businesses in order to enhance compliance with Australian workplace laws and regulations in relation to foreign worker rights and obligations.
9. To protect the public finances of Australia by aiming to detect, investigate and prosecute contraventions of taxation laws arising from, or in connection with, the exploitation of vulnerable workers.

Governance

10. Oversight to Taskforce Cadena will be provided by the Taskforce Cadena Joint Management Group (JMG). The JMG will meet at least bi-monthly and comprise the following parties:
 - AC Border Management, ABF
 - AC Strategic Border Command, ABF
 - AC Investigations, ABF
 - FAS Immigration and Citizenship Policy, DIBP
 - Commander Taskforce Cadena, ABF
 - Deputy Fair Work Ombudsman, FWO
 - ED, Dispute Resolution and Compliance, FWO
 - Other observers may be invited as the JMG requires.
11. Taskforce Cadena Operational Coordination Group (OCG) will be co-led by officers from ABF/DIBP and FWO. The OCG will meet at least monthly and will comprise the following:
 - DIBP/ABF Lead – Commander Taskforce Cadena
 - FWO Lead – Executive Director, Dispute Resolution and Compliance, FWO
 - Commander Investigations, Border Operations, ABF
 - Commander Immigration Compliance, ABF
 - AS Operational Intelligence, Intelligence, DIBP
 - AS Mobility, Immigration and Citizenship Policy, DIBP
 - Executive Director, Policy Media and Communications, FWO
12. Changes to JMG and OCG membership may occur at any time with the agreement of all parties.
13. The Taskforce will operate across the border continuum and through the SBC Regional Command and FWO network utilising operational command procedures via a Concept of Operations (COO) to be developed by the Taskforce Cadena OCG.
14. The JAA will be reviewed by the JMG on a six monthly basis so as to ensure it is delivering its objectives and deliverables.

Key Taskforce Deliverables

15. Identify and investigate major targets of interest as identified by joint intelligence activities.
16. Co-ordinate existing integrity and investigative measures being progressed by the DIBP and FWO, ensuring a coordinated, strategic approach is taken to tackling the issue of visa fraud, illegal work and foreign worker exploitation nationally.

17. Establish clear and effective lines of communication and information sharing protocols with other government agencies including seeking administrative, civil, and criminal remedies jointly with partner agencies including agencies such as the AFP, Australian Crime Commission and the Australian Taxation Office.
18. Prioritise intelligence leads for targeted action through a risk-based approach whilst ensuring that overlaying FWO and DIBP macro-control strategies underpin strategic and operational planning.
19. Establish a referral process to ensure prioritised targets are subject to appropriate operational responses. Ensure operational teams are briefed thoroughly, and provide linkages to involved or interested government agencies to ensure co-ordinated action at the operational level.
20. Manage strategic communications and reporting regarding Taskforce efforts nationally, including co-ordination of media engagement and communication campaigns.

Other Agencies

21. The Taskforce will refer matters and engage with other agencies as required to assist in delivering the objectives of the Taskforce. This may include, but is not limited to the following agencies and bodies:

- Australian Federal Police;
- Australian Competition and Consumer Commission;
- Australian Crime Commission;
- Australian Taxation Office;
- Australian Transaction Reports and Analysis Centre;
- Australian Securities and Investments Commission;
- Department of Employment;
- the prescribed Phoenix Taskforce; and
- State and Territory police forces.

Personnel and Resources

22. Each party will contribute such personnel as required to be attached to the Taskforce on a permanent or adhoc basis to support the operational activities of the Taskforce. At all times each party remains the employer of the personnel they contribute to the Taskforce and will be responsible for all administrative and legal issues relating to their personnel.
23. No party will be required to maintain resourcing obligations under the JAA in the event of major and unforeseen demands on their resources and with the agreement of the JMG.

24. Each party will ensure that prior to appointment to the Taskforce its personnel are cleared to Protected level (baseline). All costs associated with the processing of security clearances will be borne by the participating agency.

Intelligence Cell

25. The Taskforce will establish an Intelligence Cell that will be staffed by relevant analysts and intelligence officers allocated by parties to the JAA.
26. The Intelligence Cell will consolidate, assess and analyse available intelligence, and engage relevant Commonwealth and State and Territory agencies, to build a comprehensive and accurate picture for the Taskforce of fraudulent and exploitative practices, including the drivers for non-compliance and will update and maintain relevant information via a centralised process.

Costs

27. Unless otherwise agreed, each agency and work area will meet the costs of their employees attached to the Taskforce, including the payment of salaries, allowances and penalties (if applicable).

Information Management and Exchange

28. The parties agree to ensure that information exchanges are undertaken consistent with relevant provisions of the Public Service Act and any other relevant legislation that applies in relation to the sharing of information relevant to Taskforce activities.

Enforcement Activity

29. Any enforcement action undertaken (be it court proceedings or otherwise) will be the responsibility of the agency with lead responsibility in relation to the offence(s) or contravention(s) being pursued.

Dispute Resolution

30. The parties agree to negotiate promptly to resolve any dispute that arises between them in connection with this JAA and the Concept of Operations.
31. In the first instances, responsibility for dispute resolution sits at the Taskforce level and then with the JMG. If unresolved, the JMG can refer matters to the senior executive of the relevant agencies.

Duration

32. The JAA will commence from the date it is signed by relevant parties and will remain in place until such time that it is mutually terminated by the agreement of all parties.

Variation


33. This JAA may only be varied with the agreement of the parties. Any amendment will be in writing. Signed by all parties and lodged with JMG. Variation will take effect as soon as they are agreed by all parties, unless otherwise indicated.

Termination

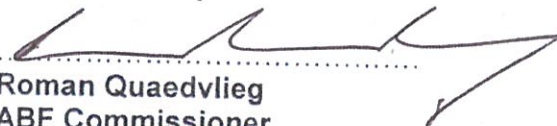
34. A party may terminate their involvement in the JAA by giving not less than 28 days written notices to the JMG. In the event that this JAA is terminated under this clause, the parties agree to negotiate in good faith arrangements to permit the parties to minimise disruptions to investigations and operational security.

Signatures


Signed for and on behalf of the Department
of Immigration and Border Protection by:


.....
Michael Pezzullo
Secretary
15/03/2016

Signed for and on behalf of the Australian
Border Force by:


.....
Roman Quaadvlieg
ABF Commissioner
11/3/16

Signed for and on behalf of the Fair Work
Ombudsman by:


.....
Natalie James
Fair Work Ombudsman
15/2/16

Released by DIBP under the
Freedom of Information Act 1982

ANNEX

to the

MEMORANDUM OF UNDERSTANDING

Between

The Department of Immigration and
Border Protection

And

The Fair Work Ombudsman

In relation to the provision of direct access to the department's
Integrated Client Service Environment (ICSE)

Released by DIBP under the
Freedom of Information Act 1982

Contents

Purpose and Recitals	2
Commencement and duration of this Annex.....	2
Status of this Annex.....	3
Personnel	3
Provision of direct online access to ICSE	3
Provision of remote access to ICSE	4
Service Delivery Support.....	4
Privacy	5
Costs	6
Security	6

Purpose and Recitals

1. This is an Annex to the Memorandum of Understanding (MOU) that was made by the Department of Immigration and Citizenship (DIAC) and the Office of the Fair Work Ombudsman (FWO) on 2 July 2013 following the appointment of FWO Inspectors as inspectors for the purposes of the *Migration Act 1958* (the 'Head MOU').
2. The purpose of this Annex is to allow Fair Work Inspectors appointed under section 700 of the Fair Work Act 2009 in the performance of their statutory duties as Migration Inspectors and FWO staff supporting their operations and investigations (including FWO IT personnel) and herein referred to as "FWO Officers", access to the Department of Immigration and Border Protection's (DIBP) Integrated Client Service Environment ("ICSE") to verify information such as which businesses are subclass 457 visa sponsors, the number of people that they sponsor and other related details such as salaries and occupations of sponsored persons.
3. This Annex sets out the arrangements between the DIBP and the FWO in relation to providing direct online access to ICSE for FWO Officers.
4. The Parties acknowledge that this initiative is in keeping with the Government's broad information sharing agenda.
5. The information provided by either party to the other party under this Annex to the Memorandum of Understanding is provided in confidence.

Commencement and duration of this Annex

6. This Annex commences on the date it is signed by the last Party to sign it, and continues to apply:
 - (a) for as long as the head MOU remains in effect; or
 - (b) Until terminated by the Parties at any time by mutual agreement, or
 - (c) Until terminated by either Party giving the other a notice of not less than 90 days.

Status of this Annex

7. The MOU, including this Annex, is a voluntary statement of intention of the Parties at the time of signing, and is not intended to create, and does not create, any legally binding obligations between the Parties, nor is it enforceable in any court or tribunal.

8. Nothing in the Head MOU or Annex will affect the statutory duties or obligations of the Parties. Any ambiguity or uncertainty arising out of this Annex is to be resolved in a way that is consistent with the relevant legislation or any other laws. Legislation and other laws, as amended from time to time, take precedence over this Annex, to the extent of any inconsistency.

9. The Parties agree to implement this arrangement in accordance with the terms and conditions set out in both the head MOU and the Annex. In the unlikely event that a conflict arises between the MOU and this annex, the relevant clauses in the Annex – being the more recent document – will take precedence over the MOU, unless otherwise agreed in writing by the MOU Managers of both parties.

Personnel

10. The MOU Managers identified in the 'Personnel' Section of the Head MOU are redefined as incumbents of the following positions:

- (a) FWO – Deputy Fair Work Ombudsman, Operations
- (b) Department of Immigration and Border Protection – National Manager, Immigration and Customs Enforcement, Investigations Division

11. The MOU Liaison Managers identified in the 'Personnel' Section of the Head MOU are redefined as incumbents of the following positions:

Role	Functions	Phone	E-mail
Director, Overseas Workers Team	Investigation referrals Requests for information Technical advice requests Joint operations	s. 22(1)(a)(ii)	s. 22(1)(a)(ii)
Director, Programme Integrity Unit	Temporary Work Sponsor Monitoring	s. 22(1)(a)(ii)	s. 22(1)(a)(ii)

12. MOU Managers and Liaison Managers will continue to confer and meet on an as-required basis.

Provision of direct online access to ICSE

13. DIBP agrees to provide direct online access to ICSE to FWO officers. It is the responsibility of the FWO to ensure that they have the appropriate systems and infrastructure to enable the access.

14. FWO will submit requests for access to ICSE using the DIBP's Other Government Agency-Access to DIBP Systems (OGA Systems Access Form), forwarded by email to: s. 22(1)(a)(ii)

15. Upon receipt of an appropriately completed and authorised OGA Systems Access Form, DIBP agrees to provide authorised FWO officers with view/read-only access to ICSE, including the Client Search Portal.

16. FWO officers will not be able to update the database directly.
17. FWO officers will be able to copy data to their desktop hard-drives and/or export data in compatible software formats.
18. FWO agrees to restrict the access and use of the information held in ICSE to authorised FWO officers who require the information for the completion of their duties.
19. Authorised Users will be subject to access controls to protect both Parties. The controls will consist of a:
 - (a) unique computer access code ("User ID"); and
 - (b) unique password.
20. When a member of FWO Officers resigns or otherwise ceases to undertake duties which require access to ICSE, FWO will Notify DIBP as soon as practicable. DIBP will promptly remove access following Notification.
21. DIBP will provide training and training modules to FWO Officers in the use of ICSE and will nominate DIBP contacts for FWO officers in the event of questions regarding usage of the ICSE system.

Provision of remote access to ICSE

22. This Annex also makes provision, if required in the future, for FWO officers to be able to access ICSE through remote means.
23. The need for remote access will be agreed by MOU Managers of both parties in writing and will be subject to:
 - (a) approval by Department of Immigration and Border Protection IT Security;
 - (b) The FWO agreeing to and meeting appropriate security protocols;
 - (c) The FWO providing appropriate hardware and software to access Department of Immigration and Border Protection systems remotely; and
 - (d) Any other protocols that are agreed to at the time.

Service Delivery Support

DIBP IT Support

24. DIBP will provide a single point of contact for all IT and telecommunications incident, problems and requests. IT Support will provide the following functions:
 - (a) Password resets;
 - (b) Reporting and tracking of technical problems with communication infrastructure;
 - (c) Providing initial Status Reports on problems logged with IT Support;
 - (d) Status Reports on requests for services;
 - (e) Providing information updates on major outages affecting departmental offices Australia-wide; and
 - (f) Resolving problems with the department's IT systems.
25. DIBP will provide IT Support 24 hours a day, 7 days a week. IT Support may be contacted via:
 - (a) Telephone: s. 22(1)(a)(ii) or
 - (b) Facsimile number: s. 22(1)(a)(ii); or

26. Once an issue is logged with the DIBP's IT Support, the issue will be allocated a severity level and the appropriate IT service provider will be responsible for fixing the issue within the service level timetable allocated to the severity level priority.

27. In instances where the FWO notifies DIBP that it is not satisfied with the service they have received from IT Support, DIBP will follow internal escalation procedures.

28. Apart from password resets, DIBP's IT Support should only be contacted by the FWO's IT Support.

29. DIBP will consult with FWO and provide necessary training for FWO Officers to use ICSE.

30. In addition, DIBP will provide the FWO with copies of relevant learning and development and operational guidance materials upon commencement of this Annex, and as they are created or updated.

FWO IT Support

31. The FWO will provide DIBP with access to FWO's IT Support to ensure the effective operation of the services between the FWO and DIBP. FWO's IT Support will perform the following functions:

- (a) Incident management from the first contact to resolution to meet escalation response and resolution;
- (b) An escalation point for calls not resolved at the first contact; and
- (c) Recording / logging of any incident received out of FWO IT business hours.

32. If a major incident is raised by FWO, DIBP IT Support will provide support, 24 hours a day, 7 days a week, until services are restored. Relevant contact details should be exchanged between FWO and DIBP IT Support service desks.

33. FWO will provide DIBP with IT Support from Monday to Friday, 8.00am to 5.00pm (AEST) weekdays excluding public holidays and the Christmas shutdown period. FWO's IT Support can be contacted via:

- (a) Telephone: s. 22(1)(a)(ii) or
- (b) Email: FWO - Service Operations Support s. 22(1)(a)(ii)

Privacy

34. The Parties acknowledge that DIBP Material contained in ICSE, which may be disclosed to FWO in accordance with this Annex, is subject to the Privacy Act.

35. The Parties acknowledge that they must comply with the Australian Privacy Principles ("APPs") (as amended from time to time) in relation to Personal Information in the Parties' possession or control in connection with this Annex.

36. FWO will, pursuant to its obligations under the Privacy Act, use Personal Information only for the authorised purposes for which it was collected. FWO will:

- (a) take all reasonable measures to ensure that Personal Information in its possession or control in connection with this Annex is protected against loss and unauthorised access, use, modification or disclosure;
- (b) comply with the APPs (as amended from time to time) and not perform an act or engage in a practice that would breach the APPs if that act was performed or that practice engaged in by an agency as defined in the Privacy Act (as amended from time to time); and

- (c) comply as far as practicable with any policy guidelines laid down by the Commonwealth or issued by the Office of the Australian Information Commissioner in relation to the handling of Personal Information.

37. Authorised Users may read, examine, reproduce, use or disclose any part of ICSE strictly for business purposes only. Authorised Users must not access records of other persons (for example relatives, associates or friends of the client) unless there is a strict business need to do so that directly relates to that person. Accessing records inappropriately is a breach of the APS Code of Conduct. Compliance with the APS Code of Conduct and any investigations into breaches will be conducted by the FWO.

38. FWO will not act as an information source for people, organisations or agencies that may request information contained in ICSE. FWO will advise any person, organisation or agency making such requests to direct their request to DIBP's Annex Manager set out in the Personnel Section of this Annex.

39. FWO will notify DIBP immediately if it becomes aware of a breach or possible breach of any of the obligations under this Annex, and will take the necessary steps to close any breach as soon as FWO becomes aware of that breach.

40. FWO understands that, when receiving DIBP Material from ICSE pursuant to this Annex, FWO becomes the custodian of that data and will treat that data as Confidential Information. FWO accepts the responsibility to ensure the prevention of unauthorised access, use, disclosure or disposal of DIBP Material received pursuant to this Annex.

41. FWO agrees that DIBP Material that is retained by FWO will be treated in accordance with the *Archives Act 1983* (Cth) and the guidelines of the relevant Government authority for the storage, disposal and archiving of Personal Information.

42. Upon receipt of an FOI request to FWO for information provided under the terms of this Annex to the Memorandum of Understanding FWO will advise DIBP.

43. FWO will process any FOI request it receives for information it holds under the terms of this Annex to the Memorandum of Understanding as it would any other FOI application it receives.

44. DIBP will provide training and written materials to FWO Officers regarding any specific privacy issues that relate to the information provided under the terms of this Annex to the Memorandum of Understanding.

Costs

45. Unless otherwise agreed between the Parties, each Agency will pay its own costs of and incidental to the preparation, negotiation, completion and performance of this Annex.

Security

46. The Parties agree to adhere to the following Commonwealth policies relating to physical, personnel and information security:

- (a) the Protective Security Policy Framework ("PSPF"); and
- (b) the Information and Communication Technology ("ICT") Security Manual ("ISM").

47. FWO shall be responsible for ensuring that DIBP Material will be kept secure and that it is protected by such security safeguards as is reasonable to prevent loss, unauthorised access, unauthorised use, modification, disclosure or other misuse, including unauthorised reproduction by any means.

48. FWO will take appropriate security measures to:

- (a) ensure that FWO's applies the principles contained in the Protective Security Framework when accessing DIBP Materials in ICSE;
- (b) restrict the use of, and access to DIBP Material to FWO Officers who require the information for the completion of their duties as Migration Inspectors and FWO Officers supporting their operations and investigations;
- (c) ensure that only FWO Officers with the appropriate security clearance and delegations will be provided with access to DIBP Material;
- (d) ensure that the DIBP Material is used only for the purposes outlined in this Annex;
- (e) restrict and monitor direct online access to ICSE; and
- (f) ensure that Authorised Users have a unique log on for the work they perform and do not share that log on.

49. If a security incident, risk, threat or vulnerability occurs in connection with access to ICSE data, FWO will Notify DIBP immediately. FWO will then prepare a written report as soon as possible providing the following information:

- (a) a description of the security incident including date, time and person(s) involved and, where appropriate, the actions taken by the agency to manage the incident to prevent its reoccurrence; and
- (b) a description of the perceived security risk and/or vulnerability.

50. FWO will also report the incident to their IT Security Advisor and Agency Security Advisor if physical or personnel security aspects are involved.

51. FWO will provide any other information which DIBP reasonably requires in relation to an incident, including providing full cooperation with DIBP during any subsequent investigation.

52. FWO will maintain records of each Authorised User who is provided with access to ICSE, including their full name, contact details, security clearance details and User ID.

53. FWO will not distribute, share or disseminate information sourced from ICSE to third parties, including to media enquiries or Ministerial offices unless:

- (a) the Material is FWO Material;
- (b) permission has been granted by DIBP;
- (c) it is being provided in accordance with a legal obligation of FWO; and/or
- (d) it is required to be produced under subpoena, notice to produce, court order, or other compulsory process.

SIGNED for and on behalf of:

**The Commonwealth Department
of Immigration and Border
Protection by:**

David Nockels,
National Manager
Immigration and Customs Enforcement Branch
Investigations Division
Immigration-Fair Work Ombudsman MOU Manager

Signed and Dated:

David Nockels 7/5/15

In the presence of (witness):

s. 22(1)(a)(ii)

Witness Signature and Date:

7/5/15

**The Office of the Fair Work
Ombudsman by:**

Michael Campbell
Deputy Fair Work Ombudsman Operations
Fair Work Ombudsman-Immigration MOU Manager

Signed and Dated:

Michael Campbell 20/5/15

In the presence of (witness):

s. 22(1)(a)(ii)

Witness Signature and Date:

20/5/15

Released by DIBP under the
Freedom of Information Act 1982