AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

FRAUD FUSION CENTRE: DATA GOVERNANCE PLAN

An Australia hostile to criminal exploitation

Purpose

Establish key principles and governance approach to the collection, use, storage and disclosure of the data exchanged within the Fraud Fusion Centre.

Context

The **Fraud Fusion Taskforce** (FFTF) is a multi-agency collaboration to strengthen the Government's approach to sharing data intelligence to assist in examining and reducing levels of fraud in the NDIS and other government payment and programs.

The ACIC led **Fraud Fusion Centre** (FFC), a centrepiece for the FFTF Intelligence Program, enables enhanced data acquisition, detection analytics and information sharing, co-located in the ACIC. The FCC is made up of expert staff from member agencies and is supported by ACIC's data analytics capability that ingests data from a variety of agencies to provide a bulk data matching capability, lead generation and intelligence support, in accordance with the FFTF **Intelligence Program** managed by the FFC and approved by the FFTF **Intelligence and Operations Committee**.

The FFTF is co-led by NDIA and Services Australia and includes the following agencies:

Aged Care Quality and Safety Comm	Dept of Education
Attorney General's Dept	Dept of Health and Aged Care
Aust Charities & Not for Profits Comm	Dept of Social Services
Aust Criminal Intelligence Comm	Dept of Veterans Affairs
AFP	National Disability Insurance Agency
ASIC	Nat'l Indigenous Aust Agency
Aust Skills Quality Authority	NDIS Quality & Safeguards Comm
ATO	Office Registrar of Indigenous Comm
AUSTRAC	Prof Services Review Agency
Cwlth Dir of Pubic Prosecutions	Services Australia
Dept of Empl & Workplace Relations	Tax Practitioners Board

Legislation and Policies

The handling of exchanged information across all FFT agencies will comply with all laws and policies that apply to the respective agency, including:

- *National Disability Insurance Scheme Act 2013 (Cth)*
- *Privacy Act 1988 (Cth)*
- *Public Governance, Performance and Accountability Act 2013 (Cth)*
- *Australian Crime Commission Act 2002 (Cth)* (ACC Act)
- *Archives Act 1983 (Cth)*
- Australian Government Protective Security Policy Framework
- Australian Government Information Security Manual.

While not subject to the *Privacy Act 1988*, the ACIC ensures that, to the extent that is reasonably compatible with the effective performance of its functions, it complies with Australian Privacy Principles. *See ACIC Information Handling Protocol for further information.*

Objectives

- Build understanding across FFC members and their agencies of FFC data collection, use and dissemination requirements and roles and responsibilities.
- Build a culture of trust and data sharing within the FFC and their agencies to support effective delivery of Government objectives.
- Member agencies provide regular and timely access to trusted, accurate and reliable data, allowing its ongoing use and reuse.
- Ensure data is shared and managed in line with whole of Government standards and assist agencies in meeting their legislative and regulatory obligations.
- Support the FFC and their agencies to minimise risks around data, whilst extracting the maximum value from it.
- Establish appropriate mechanisms to support rapid and regular sharing of data and information by FFC agencies and external partners.

Data Lifecycle Governance

Data acquisition

- Data will be collected, used, stored and disclosed in accordance with the FFT Intelligence Program, approved by the Intelligence and Operations Committee and managed by the FFC. Data collected is to support the FFT in identifying, understanding, targeting, preventing, or disrupting serious and organised crime (SOC) groups operating within identified Government funded programs. s 37(2)(b), s 47E(d) [redacted] Further, data acquired will assist the ACIC more broadly in its functions of collecting, analysing and disseminating criminal information and intelligence under the ACC Act section 7A(a).
- The data collected and stored by the ACIC is consistent with any use, handling and disclosure restrictions agreed with the provisioning agency. The contributing agency is responsible for articulating any use, handling, and disclosure restrictions to the ACIC, this includes public interest or Privacy Impact Assessment considerations. This will assist and ACIC disclosure delegate to assess the requirements of the disclosure test in section 59AA of the ACC Act. Agencies are also responsible for ensuring their data is timely, accurate and reliable and can be lawfully provided to the ACIC.

Data storage, use and analysis

- Predominately, the ACIC data analytics capability will utilised across the data s 37(2)(b), s 47E(d) [redacted] and use other analytical capabilities as required. The results will be provided to the FFC to be used and analysed for the purposes of the FFT. s 37(2)(b), s 47E(d) [redacted] The data may be held by ACIC to identify any further or future engagement with serious organised crime entities in the performance of ACIC's broader statutory functions, unless otherwise restricted by the contributing agency or FFTF.
- The ACIC is subject to a robust accountability framework to ensure that it uses its statutory powers set out in the ACC Act responsibly, effectively and in accordance with the law. s 37(2)(b), s 47E(d) [redacted] ACIC system use is audited and strictly managed. Substantial protection currently afforded to sensitive information held by the ACIC including secrecy provisions, legislative restrictions on disclosure of ACIC information, examiner's confidentiality directions imposed by ACIC examiners, and comprehensive external oversight of the ACIC's activities.

Information Disclosure

- Only ACIC Members of Staff, when performing their role, are allowed to have access to ACIC data and information, unless the data/ information is authorised for disclosure to an entity.
- In accordance with the ACIC Information Disclosure regime, ACIC members of staff (including secondees and members of ACIC Board-approved task forces) may disclose data and information to external agencies (including their home agencies) to assist in their agency's functions of protecting public revenue and managing risk to the financial sustainability of government programs. However, it must be authorised for disclosure by the ACIC CEO or SES delegate in accordance with the ACIC's information disclosure regime under the ACC Act. Members and agencies must not otherwise disclose or communicate ACIC information without the prior written permission of the ACIC. For example, ACIC members of staff cannot:
  - Disclose ACIC information to their home agency supervisor (unless the home agency supervisor is performing a role in the FFC), this includes a member's own agency information that is in the possession of the ACIC.
  - Provide access to ACIC systems and ACIC information to colleagues in their home agency.
  - Use ACIC information to give additional context, providing credibility to information within their home agency.
- ACIC information is only to be used for intelligence purposes. Any information to be relied upon to initiate criminal or administrative activity should be directly sourced from the owning Agency. The nature of ACIC criminal intelligence is such that the accuracy of the information is contestable. The ACIC takes reasonable steps to assess the reliability of source and other information in its criminal intelligence products and applies a reliability rating prior to disclosure. However, the ACIC cannot guarantee the accuracy, completeness, relevance or currency of criminal intelligence.
- The ACIC will not otherwise disclose or communicate agency information without prior written permission of the relevant agency.

Manage

- All agencies must comply with security policies, guidelines and advisories in the relevant agency Protective Security Management Framework, the Australian Government Protective Security Policy Framework, and Australian Government Information Security Manual for the purposes of the FFC. They will notify in writing as soon as possible of any breaches to the ACIC.

Supporting Documentation

- FFTF Memorandum of Understanding
- Terms of Reference: FFT Inter-Departmental Committee; FFT Strategic Prevention Committee; and, FFT Intelligence and Operations Committee
- FFTF Data Governance Strategy
- FFTF Intelligence Program
- FFC Collection Plan
- FFC Data Model and Use Cases
- FFC Data Concepts of Operations
- ACIC Information Handling Protocol
- ACIC Fact Sheet: ACIC Members of Staff
- ACIC Fact Sheet: Use and Disclosure of Information
- Bi-lateral Memorandums of Understanding; Privacy Impact Assessments; Public Interest Certificates (as developed)

Key ACIC Governance Concepts

ACIC Information. All data supplied to the ACIC by its member agencies will become 'ACC information' under the ACC Act. The definition is broad and does not distinguish between classified and unclassified information. This importantly includes information given to the ACIC by other Commonwealth, State and Territory agencies.

ACIC Member of Staff. Any person who is engaged as an ACIC secondee or member of the ACIC Board approved Task Force Reston* will become an ACIC Member of Staff and have information handling and secrecy obligations under the ACC Act. Members may only use 'ACC information' for ACIC's purposes and in accordance with any restrictions placed on it by the source agency. Should a secondee or Board-approved taskforce member wish to make the information available to their home agency, seek formal approval for 'information disclosure'. *See External Agency Member of Staff Factsheet for further information.*

**The Fraud Fusion Taskforce is not an ACIC Board-approved task force. Task Force Reston, approved by the ACIC Board on 20 April 2023, interacts with and supports the FFTF and the FFTF Intelligence Program managed by the FFC where the objectives of each align (noting Task Force Reston operates under the ACC Act independently of the FFTF).*

ACIC Information Disclosure. ACIC Members of Staff have information and handling and secrecy obligations under the ACC Act. Section 51 of the ACC Act prohibits the making a record of, divulging or communicating any information acquired in the course of duties, except as provided for under the ACC Act or a prescribed 'Relevant Act' - to do so could be considered a breach of the secrecy provision, which is punishable by imprisonment for up to 2 years or 120 penalty units, or both. All disclosures must be authorised by the ACIC CEO or an ACIC SES delegate, even if the information is unclassified, and must meet the legislative tests set out in the ACC Act and/or other relevant Act. *See External Agency Information Disclosure Factsheet for further information.*

Released under Freedom of Information Act 1982 (Cth)

Version v1.1 – April 2025 (Visio: 22/199069; PDF: 23/107876)

DOCUMENT 2

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

STRATEGIC ANALYSIS AND OUTREACH BRANCH

s 37(2)(b) USER GUIDE – Fraud Fusion

MAY 2025

Released under the Freedom of Information Act 1982 (Cth)

CONTENTS

Proof of Concept - s 37(2)(b) 3

Background 3

Fraud Fusion Taskforce 3

The Data 4

Data Background – Fraud Fusion 4

Access to the Data - s 37(2)(b) 5

User Groups 5

Classification of Data 6

Use of Data 6

USER Guidelines 6

Accessing Interface and Acknowledging Terms and Conditions 6

intelledox and dissemination of information 7

Intelledox and Disseminations 7

s 37(2)(b), s 47E(d)

Review of Proof of Concept/ auditing 9

related documents 9

Key Contacts 10

Contact Officer 10

Record of approval 10

Record of amendment 10

Released under the Freedom of Information Act 1982 (Cth)

s 37(2)(b), s 47E(d)

[redacted]

Background

s 37(2)(b), s 47E(d)

[redacted]

Fraud Fusion Taskforce

The Fraud Fusion Taskforce (FFTF) is a multi-agency collaboration to strengthen the Government's approach to sharing data intelligence to assist in examining and reducing levels of fraud in the NDIS and other government payment and programs.

The ACIC led Fraud Fusion Centre (FFC), a centrepiece for the FFTF Intelligence Program, enables enhanced data acquisition, detection analytics and information sharing, co-located in the ACIC. The FCC is made up of expert staff from member agencies and is supported by ACIC's data analytics capability

Released by the Freedom of Information Act 1982 (Cth)

that ingests data from a variety of agencies to provide a bulk data matching capability, lead generation and intelligence support, in accordance with the FFTF Intelligence Program managed by the FFC and approved by the FFTF Intelligence and Operations Committee. See FFC Data Governance Plan - v1.1 April 2025 - updated participating agencies for further information.

The FFTF is co-led by NDIA and Services Australia and includes the following agencies as at 12 March 2025:

- AGED CARE QUALITY AND SAFETY COMMISSION
- ATTORNEY-GENERAL'S DEPARTMENT
- AUSTRALIAN CHARITIES AND NON FOR PROFITS COMMISSION
- AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION (ACIC)
- AUSTRALIAN FEDERAL POLICE (AFP)
- AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION (ASIC)
- AUSTRALIAN SKILLS QUALITY AUTHORITY
- AUSTRALIAN TAXATION OFFICE (ATO)
- AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE (AUSTRAC)
- COMMONWEALTH DIRECTOR OF PUBLIC PROSECUTIONS (DPP)
- DEPARTMENT OF EMPLOYMENT AND WORKPLACE RELATIONS
- DEPARTMENT OF EDUCATION
- DEPARTMENT OF HEALTH AND AGED CARE
- DEPARTMENT OF SOCIAL SERVICES
- DEPARTMENT OF VETERANS' AFFAIRS
- NATIONAL DISABILITY INSURANCE AGENCY
- NATIONAL INDIGENOUS AUSTRALIANS AGENCY
- NDIS QUALITY AND SAFEGUARDS COMMISSION
- OFFICE OF THE REGISTRAR OF INDIGENOUS CORPORATIONS
- PROFESSIONAL SERVICES REVIEW AGENCY
- SERVICES AUSTRALIA
- TAX PRACTITIONERS BOARD

THE DATA

Fraud Fusion Task Force Integrated Data Holdings

1. The Data collected by the ACIC is used, stored and disclosed in accordance with the FFT Intelligence Program, approved by the Intelligence and Operations Committee and managed by the FFC. Data collected aims to support the FFT in identifying, understanding, targeting, preventing, or disrupting serious and organised crime (SOC) groups operating within identified Government funded programs.
2. s 37(2)(b), s 47E(d) [redacted]

Released under the Freedom of Information Act 1982 (Cth)

s 37(2)(b), s 47E(d) Data collected will assist the ACIC more broadly in its functions of collecting, analysing and disseminating criminal information and intelligence under the ACC Act section 7A(a).

3. The data collected and stored by the ACIC is consistent with any use, handling and disclosure restrictions agreed with the provisioning agency. The contributing agency is responsible for articulating any use, handling, and disclosure restrictions to the ACIC, this includes public interest or Privacy Impact Assessment considerations. This will assist the ACIC disclosure delegate to assess the requirements of the disclosure test in section 59AA of the ACC Act. Agencies are also responsible for ensuring their data is timely, accurate and reliable and can be lawfully provided to the ACIC.
4. s 37(2)(b)
5. Any person who is engaged as an ACIC secondee or member of the ACIC Board approved Task Force Reston[1] will become an ACIC Member of Staff and have information handling and secrecy obligations under the ACC Act. Members may only use 'ACC information' for ACIC's purposes and in accordance with any restrictions placed on it by the source agency. Should a secondee or Board-approved taskforce member wish to make the information available to their home agency, seek formal approval for 'information disclosure'.

s 37(2)(b), s 47E(d)

User Groups

11. The Proof-of-Concept User Groups include:
    a. User – MoS who have been granted access to use .
    b. Developers – This group will include A/ Director Advanced Analytics Data and MoS of the Advanced Analytics Team.

[1]The Fraud Fusion Taskforce is not an ACIC Board-approved task force. Task Force Reston, approved by the ACIC Board on 20 April 2023, interacts with and supports the FFTF and the FFTF Intelligence Program managed by the FFC where the objectives of each align (noting Task Force Reston operates under the ACC Act independently of the FFTF).

Released under the Freedom of Information Act 1982 (Cth)

c. Administration - This group will include Director Data Analytics and Senior Specialist Data Engineering.

Classification of Data

12. The classification of the data as well as the caveats placed on its use will remain as per original classification from Taskforce Member Agencies at time of receipt.
13. The output of the data after the value-add and analysis has been conducted in [redacted] will require its own classification marking.
14. If combinations of data are being used to inform a new Intelligence Product, as a minimum, the highest Protective marking of the data used will need to be the new classification marking – for example is datasets containing Official and Protected information and merged and utilised to create a product, this product will need to be classified at a Protected level.

Use of Data

[redacted]

USER GUIDELINES

Accessing Interface and Acknowledging Terms and Conditions

16. When logging on to [redacted]
17. The data is to be used for Intelligence Purposes only.
18. User will choose the one application appropriate for their purpose.
19. [redacted] – user will have to Agree to the Terms of Conditions of Access to the application.
20. Terms and Conditions will read as follows:

Released under Freedom of Information Act 1982 (Cth)

WARNING

Access to this system is restricted due to the sensitive nature of the material it contains.

Unauthorised access to systems or disclosure of deformation may be a breach of the ACIC Code of Conduct and / or a criminal offence. If you need an account, please contact s 47E(d) [redacted] @acic.gov.au

-

The system you are accessing may contain Protected Information as defined in the Surveillance Devices Act 2004. You must not use or communicate Protected Information except for a purpose connected with an ACIC operation / investigation, or on the advice of an ACIC Legal Officer.

-

The system you are accessing contains information from Member Agencies of the Fraud Fusion TaskForce (FFTF). The data collected and stored by the ACIC is consistent with any use, handling and disclosure restrictions agreed with the contributing agency. The contributing agency is responsible for articulating any use, handling, and disclosure restrictions to the ACIC, this includes public interest or Privacy Impact Assessment considerations. These restrictions on use and disclosure will assist in the disclosure requirements under section 59AA of the ACC Act.

-

By clicking on the 'OK' button I acknowledge that:

1. I am aware of, and must comply with, ACIC policies, procedures and relevant legislation on access to and disclosure of information by the ACIC, and in particular s51(2) of the Crime Commission Act 2002.
2. I am aware of, and must comply with, ACIC policies, procedures and relevant legislation on the appropriate use of technology. This includes not providing others with access to your account or sharing information for which they would otherwise not have access.
3. My use of ACIC systems and ACIC information can be logged, monitored and audited.

INTELLEDOX AND DISSEMINATION OF INFORMATION

Intelledox and Disseminations

21. Only ACIC Members of Staff, when performing their role, are allowed to have access to ACIC data and information, unless the data/information is authorised for disclosure to an entity.

Released under the Freedom of Information Act 1982 (Cth)

22. In accordance with the ACIC Information Disclosure regime, ACIC members of staff (including secondees and members of ACIC Board-approved task forces) may disclose data and information to external agencies (including their home agencies) to assist in their agency's functions of protecting public revenue and managing risk to the financial sustainability of government programs. However, it must be authorised for disclosure by the ACIC CEO or SES delegate in accordance with the ACIC's information disclosure regime under the ACC Act. Members and agencies must not otherwise disclose or communicate ACIC information without the prior written permission of the ACIC.
23. The ACIC data analytics capability will utilised s 37(2)(b), s 47E(d) [redacted] The results will be provided to the FFC to be used and analysed for the purposes of the FFT. s 37(2)(b), s 47E(d) [redacted]
24. The data may be held by ACIC to identify any further or future engagement with serious organised crime entities in the performance of ACIC's broader statutory functions, unless otherwise restricted by the contributing agency or FFTF.
25. The ACIC will not otherwise disclose or communicate agency information without prior written permission of the relevant agency. Specific to the data received by The Fraud Fusion Taskforce, each agency member has its own legal advice and/or caveats placed on the data they provide. A complete breakdown of this list of Agencies and requirements can be found Fraud Fusion Centre – Data Analytics Home Page - Fraud Fusion Centre – Data Analytics - ACIC
26. If the new Product contains information derived from the original data provided by Taskforce members, the ACIC will seek permission for the use of that product if not already authorised during the original disclosure.
27. ACIC Members of Staff have information and handling and secrecy obligations under the ACC Act. Section 51 of the ACC Act prohibits the making a record of, divulging or communicating any information acquired in the course of duties, except as provided for under the ACC Act or a prescribed 'Relevant Act' - to do so could be considered a breach of the secrecy provision, which is punishable by imprisonment for up to 2 years or 120 penalty units, or both.
28. All disclosures must be authorised by the ACIC CEO or an ACIC SES delegate, even if the information is unclassified, and must meet the legislative tests set out in the ACC Act and/or other relevant Act. See External Agency Information Disclosure Factsheet for further information Record 23/112483: External Agency Fact Sheet - ACIC Board Task Forces and Information Disclosure.
29. The disseminations of ACIC products derived through the use of s 37(2)(b), s 47E(d) will be treated as per any other product disseminated by the agency, and apply the standard ACIC product caveat.
30. The Disclosure checklist procedures will need to be followed as per agency protocol. As a guide please see Information Disclosure Quick Reference Guide A3_v02.

Released under the Freedom of Information Act 1982 (Cth)

s 37(2)(b), s 47E(d)

REVIEW OF PROOF OF CONCEPT/ AUDITING

38. Auditing of logs for the duration of the proof of concept will be conducted by A\Director Advanced Analytics (Data) and Director Analytics Development, Hub Strategic Analysis & Outreach Branch.
39. A review of the Proof of Concept will take place after its cease date of 18 December 2025 by A\Director Advanced Analytics (Data) and Director Analytics Development, Hub Strategic Analysis & Outreach Branch.

RELATED DOCUMENTS

s 47E(d)

Record 23/107876: FFC Data Governance Plan - v1.1 April 2025 - updated participating agencies

Fraud Fusion Centre – Data Analytics Home Page - Fraud Fusion Centre – Data Analytics - ACIC

s 22(1)(a)(ii)

Released under Information Act

s 37(2)(b), s 47E(d)

KEY CONTACTS

s 47E(d) @acic.gov.au

Contact Officer

s 22(1)(a)(ii)

Job Title	A\Director Advanced Analytics (Data)
Branch	Strategic Analysis and Outreach Branch

Record of approval

Version	Name	Title	Date	Next review
1.0	s 22(1)(a)(ii)	A\Director Advanced Analytics (Data)	TBA	1 year from approval date, or as required

Record of amendment

Version	Name	Amendments made	CM link + Revision number	Date
1.0	s 47E(d)	Original Draft	Record 25/110183: Intelligence - SAO - Advanced Analytics - s 47E(d), s 37(2)(b)	1 year from approval date, or as required

Released under the Freedom of Information Act 1982 (Cth)

DOCUMENT 3

Fraud Fusion Taskforce
Memorandum of Understanding

Dated: 25 May 2023

2. Definitions

In this MOU, the following words, expressions and acronyms have the following meanings unless a contrary intention appears:

Words and expressions	Meaning
ACC Act	*Australian Crime Commission Act 2002* (Cth)
[redacted] s 22(1)(a)(ii)	
ACIC information	Has the same meaning as 'ACC information' given in s4(1) of the ACC Act: information that is in the ACIC's possession
[redacted] s 22(1)(a)(ii)	
Confidential information	Any information, including personal information, relating to the business, affairs or clients of a Party which is confidential in nature and the other knows (or should reasonably know) is confidential and includes data/information shared between the parties of the Fraud Fusion Taskforce. It can include anything that has been acquired, developed or made available to any of the Parties in the course of this MOU. It includes, but is not limited to, information: • specifically identified as confidential in the MOU or which contains confidential markings; • where disclosure would cause unreasonable detriment to the owner of the information or another party; or • where the information was provided under an understanding that it would remain confidential
[redacted] s 22(1)(a)(ii)	
Data Governance Plan	Documented data sharing and security framework for the Fraud Fusion Taskforce
[redacted] s 22(1)(a)(ii)	

Released under Freedom of Information Act 1982

[redacted]

Eligible Data Breach	Has the meaning given under s26WE(2) of the *Privacy Act 1988* (Cth)

[redacted]

Fraud Fusion Intelligence Program	Managed by the ACIC under an ACIC Program Head - Program involving the ACIC collecting criminal intelligence and analysing and crossmatching data from numerous sources (including but not limited to the NDIA, Services Australia, NQSC, ATO, AFP, ASIC, AUSTRAC, DoHA, DoE and DEWR) to provide strategic and tactical intelligence advice to the Fraud Fusion Taskforce and its members to address the purpose and objectives of the Fraud Fusion Taskforce

[redacted]

Rele

s 22(1)(a)(ii)

7. Governance and Responsibilities

s 22(1)(a)(ii)

2) All Parties agree to share data and intelligence and contribute to the Fraud Fusion Taskforce in accordance with this MOU to the extent of any applicable legislative framework and subject to any legislative restrictions, conditions imposed under subclause 13(4)(a), and any further terms of agreement (such as outlined in a bi-lateral MOU or PIC) between two or more of the Parties.

s 22(1)(a)(ii)

[redacted]

7) A Fraud Fusion Intelligence Program will be established and independently managed by the ACIC. The Fraud Fusion Intelligence Program will be led by a Program Head, who will be an appointed ACIC SES officer. The Fraud Fusion Intelligence Program will:

[redacted] s 22(1)(a)(ii)

e) Act as the Fraud Fusion Taskforce's centerpiece for intelligence collection, correlation, analysis and dissemination.

[redacted] s 22(1)(a)(ii)

Rel

[redacted]

14. Data, Information sharing and security

1) Subject to any relevant legislation, Government policy, and responsible staff (Fraud Fusion Taskforce Officers) having an adequate Security Clearance and appropriate 'Need to Know', each of the Parties undertakes to share information (including confidential information and intelligence) relevant to the achievement of the objectives and intent of the Fraud Fusion Taskforce. This will occur in accordance with the agreed Taskforce Data Governance Plan (to be endorsed by the IDC) and other information management agreements between agencies that are Parties to this MOU.

2) This may include staff of the Parties being engaged as members of the staff of the ACIC under the ACC Act, to assist in the performance of the Fraud Fusion Centre and Fraud Fusion Intelligence Program.

3) The Parties acknowledge that collecting, recording and sharing, or otherwise handling, information pursuant to this MOU may involve information that is subject to the Privacy Act and/or secrecy laws that each of the Parties must comply with, such as the protected information provisions in the *National Disability Insurance Scheme Act 2013* (Cth) (NDIS Act) or any caveats placed on the information by the Party providing it.

4) The Parties agree not to collect, use or disclose information, to another Party or any third party, unless it is consistent with legislative obligations and agreements or arrangements with the originating or disclosing agency.

5) The Parties agree to comply with the Australian Government Protective Security Policy Framework (PSPF) and the Information Security Manual in respect of information obtained and created for the purposes of the Fraud Fusion Taskforce.

6) All information tabled with the IDC, other Taskforce committees and any working groups will be treated as confidential and given the appropriate markings under the PSPF.

7) The Parties will be responsible for:

   a) Ensuring appropriate information and physical security measures are in place to protect any information provided by another agency from unauthorised access or disclosure.

   b) Individually and collectively considering the nature of data sharing under the Fraud Fusion Taskforce and addressing the requirement to have a Privacy Impact Assessment conducted under s12 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017*.

   c) Restricting any person from accessing information provided by an agency unless that person is legally entitled to do so.

   d) Complying with any conditions, restrictions or caveats imposed by a disclosing agency in respect of the use, handling, and disclosure of that information.

   e) Complying with all relevant State, Territory and Commonwealth legislation.

   f) Obtaining input and/or clearance from the agency from which the information originated to the Fraud Fusion Taskforce if any uncertainty exists in relation to the use or further dissemination of the information.

Released under the Freedom of Information Act 1982 (Cth)

8) The Parties shall ensure that any of their Fraud Fusion Taskforce Officers (authorised to access information obtained from another agency) shall not record, disclose, or otherwise communicate such information except in the performance of their official duties and subject to any privacy or secrecy laws, this MOU and the agreed data governance arrangements for the Fraud Fusion Taskforce.

9) Subject to subclauses 8(3) and 8(4), if one of the Parties becomes aware that information received under the Fraud Fusion Taskforce's arrangements or pursuant to this MOU becomes the subject of a lawful request or requirement for access, production or disclosure (for example in the form of a subpoena, summons, notice to produce, or freedom of information request), the recipient of the information will immediately, as permitted by law:

   a) Advise the agency that provided the information ('originating agency') of the request for the information.

   b) Promptly notify the originating agency and seek advice from the originating agency, which must respond in a reasonable timeframe, on the implications of disclosing the information and the most appropriate course to pursue in responding to the request.

   c) Keep the IDC Co-Chairs informed of the request (subclause 8(4)).

   d) Take all reasonable steps, subject to the requirements of the relevant legislative framework for disclosure, to ensure that the concerns of the originating agency are considered before the information is disclosed.

10) **ACIC Information and Members of Staff**

   a) Information in the possession of the ACIC ('ACIC Information'), including information provided to it by other agencies, is subject to use and disclosure restrictions under the ACC Act, and the ACIC's Information Handling Protocol[1].

   b) Staff engaged as members of the staff of the ACIC (i.e., for the purpose of assisting the ACIC's Fraud Fusion Centre and Fraud Fusion Intelligence Program), are subject to the secrecy provision at section 51 of the ACC Act and must comply with the ACIC's information disclosure legislative and policy framework.

   c) All information obtained by Fraud Fusion Taskforce Officers, in the performance of their duties as members of the staff of the ACIC, will be considered ACIC Information.

11) **Cyber security incidents**

   a) If a Party suspects that there may have been an Eligible Data Breach in relation to any Personal Information held by it in relation to the Fraud Fusion Taskforce, the party must:

      i) immediately report it to the IDC Co-Chairs or their representatives and provide a written report within three (3) business days

      ii) carry out an assessment in accordance with the requirements of the *Privacy Act 1988* (Cth).

   b) Where a Party is aware that there has been an Eligible Data Breach in relation to the Fraud Fusion Taskforce, the Party must:

      i) take all reasonable action to mitigate the risk of the Eligible Data Breach causing serious harm to any individual to whom the Personal Information relates

      ii) take all other action necessary to comply with the requirements of the *Privacy Act 1988* (Cth) and relevant confidentiality, secrecy and cyber security provisions within legislation, as relevant to each government program administered by individual Parties, including as outlined in agreements between the respective Parties

[1] Available online: https://www.acic.gov.au/sites/default/files/2020-08/information_handling_protocol.pdf

Released under the Freedom of Information Act 1982 (Cth)

iii) take any other action as reasonably requested by an IDC Co-Chair or directed by the IDC, as permitted by law.

c) Sub-clauses 14(11)(a) – (b) only apply to the ACIC to the extent that ACIC's compliance with these obligations is reasonably consistent with the performance of ACIC's functions and the exercise of its legislative powers.

Note: Subclause 14(11)(c) acknowledges that ACIC's acts and practices are not subject to the operation of the *Privacy Act 1988* (Cth).

d) Further data breach reporting and management arrangements will be outlined in the Data Governance Plan.

15. Taxation information

1) The disclosure of ATO protected information is prohibited, except in certain specified circumstances[1]. An exception to this general prohibition permits disclosure to a Taskforce Officer[2] of a prescribed taskforce if the disclosure is made for, or in connection with a purpose of the prescribed taskforce[3].

2) The Fraud Fusion Taskforce is a 'prescribed taskforce' under Regulation 67 of the *Taxation Administration Regulations 2017*.

3) ATO protected information means information that was disclosed or obtained pursuant to a Commonwealth taxation law which relates to the affairs of an entity and identifies or is reasonably capable of being used to identify the entity[4].

[redacted]
s 47E(d)
s 22(1)(a)(ii)

Released under the Freedom of Information Act 1982 (Cth)

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Fraud Fusion Taskforce

OFFICIAL

Taskforce Intelligence Program – Operating Model

s 22(1)(a)(ii)

Re[illegible] from of [illegible]

Intelligence Collection and Analysis Capabilities supporting the TIP

Collection and analysis of information, data and intelligence holdings of Taskforce agencies

Taskforce agencies currently hold large volumes of information, data and intelligence that will, or could, be relevant to the work of the TIP. Relevant information, data and intelligence will be brought into the ACIC via lawful disclosure pathways. The Fraud Fusion Centre Data Tank, managed by the ACIC Data Analytics Branch, is the physical location where information, data and intelligence will be brought together to enable its exploitation in furtherance of the Taskforce.

s 37(2)(b), s 47E(d)

Proactive Intelligence Collection Powers and Capabilities

As part of its work under the *Special ACIC Operation Determination (Serious Financial Crime) 2022*, the ACIC has a variety of specialist powers and capabilities that can be used to collect intelligence and evidence in support of the TIP. The ACIC can only exercise these powers and capabilities in furtherance of its own purposes; however, the purposes of the ACIC and the priorities of the TIP will have significant overlap. These capabilities include:

- Human Source recruitment and management (including proactive deployment under Commonwealth Controlled Operations legislation)
- Telecommunications data collection and analysis
- Telecommunications and data interception

[1] For example, identification that the Department of Education, NDIA, Australian Charities and Not-for-profit Commission and Australian Skills and Quality Assurance are all investigating the same network for different but interconnected fraud, allowing for information sharing and coordination of operational effort.
[2] For example, entity on the National Gangs List who is suspected of fraud against a Government program where the AFP or State/Territory Police would be interested in undertaking operational effort.
[3] This line of effort is about utilising the analysis of information, data and intelligence to identify the most appropriate Taskforce targets of the future.
[4] For example, NDIS providers that are not compliant with their taxation obligations as identified by the ATO.
[5] For example, identifying entity that has been removed from one program due to serious non-compliance and is now operating in another program without the previous conduct having been factored into risk mitigation.

Released under the Freedom of Information Act 1982 (Cth)

- Computer Access
- Surveillance devices (including audio, optical and tracking devices)
- Coercive powers, including examination of witnesses, notices to produce and *Australian Crime Commission Act 2002* Section 22 search warrants
- Physical surveillance.

s 37(2)(b), s 47E(d)

s 22(1)(a)(ii)

Rel

FRAUD FUSION CENTRE: DATA MODEL

s 37(2)(b), s 47E(d)

BACKGROUND: FFC OBJECTIVES

The FFC seeks to cause systemic change within the ecosystem surrounding GP&Ps to minimise fraud and ensure that money goes to those entities to which it is meant to go. The FFC will achieve systemic change on a continuum from tactical to strategic through supporting the following outcomes:

- Fraud Deterrence (through criminal prosecution outcomes and alternative disruption – to be referred to collectively as "enforcement outcomes" - and a communications plan);
- Enhanced Risk Identification and Mitigation; and,
- Policy change.

FFC agencies and other GP&P currently hold large volumes of information, data and intelligence that will or could be relevant to meeting FCC TF outcomes. It is proposed that relevant information, data and intelligence will be brought together in the ACIC via lawful disclosure pathways. The data model will play a key role in ensuring the lawful exchange and use of data.

The FFC data holdings, managed by the ACIC Data Analytics Branch, is the physical location where data and intelligence will be brought together to enable its exploitation in furtherance of the FFT.

s 37(2)(b), s 47E(d)

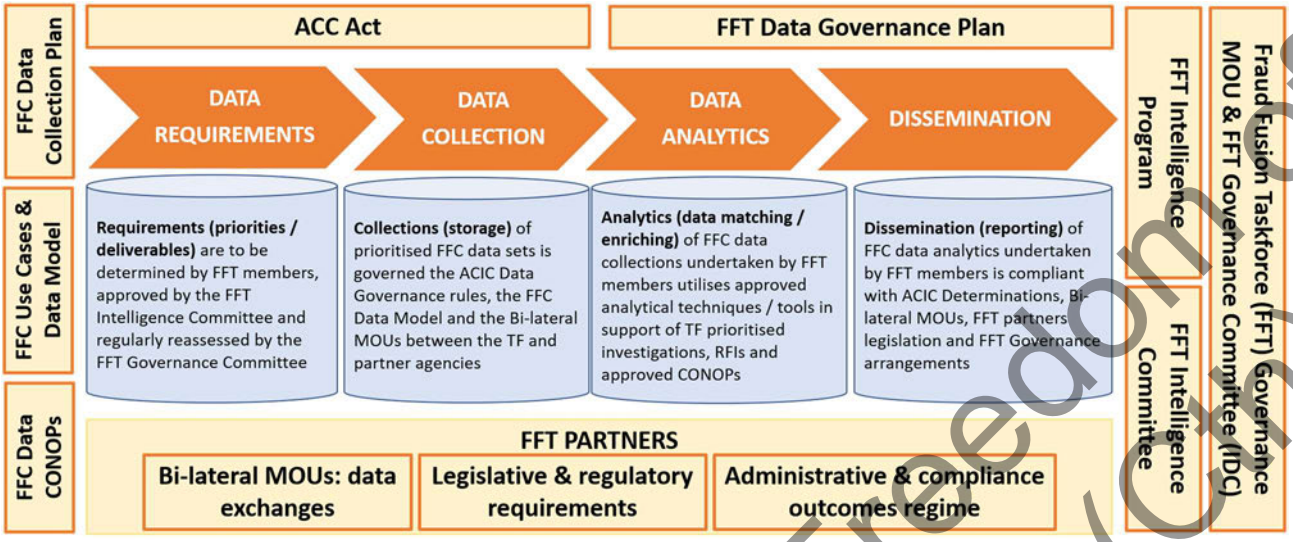
DATA GOVERNANCE ACROSS THE INTELLIGENCE CYCLE

Strong data governance across the whole intelligence cycle is essential for ensuring the lawful exchange and use of data in detecting fraud within GP&Ps. The FFT Data Governance Plan provides the overarching set of arrangements across the whole intelligence cycle. Other artefacts play key roles, depending on the stage of the process, which is broken down as follows:

1. Determination of **data requirements** to meet FFC objectives;
2. Undertaking of **data collection** s 37(2)(b), s 47E(d)
3. Performing **data analytics** across data sets;
4. **Disseminating** the outputs of the data analytics s 37(2)(b), s 47E(d)

Released under the Freedom of Information Act 1982 (Cth)

The following diagram provides a list of the key artefacts – documents, committees, legal frameworks - underpinning data governance across the whole intelligence cycle.



Definitions:

ACC Act 2002 – *provides the legal framework underpinning the collection, correlating, analysis and dissemination of data by ACIC members & secondees to the FFC*

s 37(2)(b), s 47E(d)

FFC Use Cases & Data Model – *FFC approved model governing the collection, storage, enrichment, entity matching, access, analysis and dissemination of data*

FFT Data Governance Plan – *overarching set of data governance arrangements across all ACIC data holdings linked to activities of the FFT*

FFT Governance Committee (IDC) – *governance arrangements of the FFT that are approved, managed and updated by a Band-2 TF Governance Committee (IDC) and codified within a MOU*

FFT Intelligence Committee - *the Director-level committee of FFT members governing the FFT intelligence program and determining intelligence and operational priorities*

FFT Intelligence Program – *the intelligence program in the Commonwealth fraud space to: improve fraud deterrence; enhance risk identification; and, encourage policy change*

FFT Partners Administrative & Compliance Outcomes Regime – *FFT administrative and compliance rules governing the use of FFT disseminated intelligence holdings for internal outcomes/actions*

FFT Partners Bi-lateral MOUs – *bi-lateral partner arrangements with the FFT providing specific rules governing the collection, analysis and dissemination of data provided to the FFT*

FFT Partners Legislative & Regulatory requirements – *FFT partner legislative and regulatory rules governing the provision of data to the FFT and the use of FFT disseminated intelligence holdings*

FFT prioritised investigations – *investigative activities to support law enforcement outcomes approved and prioritised through the FFT Intelligence Committee*

FFT RFIs - *activities to support the analysis and dissemination of intelligence approved and prioritised through the FFT Intelligence Committee*

DATA GOVERNANCE: KEY PRINCIPLES ACROSS THE INTELLIGENCE CYCLE

This section will provide details on the role all of the artefacts in delivering data governance across the intelligence cycle.

Data Requirements (priorities / deliverables) are to be determined by FFC members and fit within the FFC Intelligence program. They are approved by the FFT Intelligence Committee and regularly reassessed by the FFT Governance Committee. The data model will provide a set of use cases to assist in capturing the key data requirements.

Released under the Freedom of Information Act 1982 (Cth)

Data Collections (storage) of prioritised FFC data sets is governed by the FFT Data Governance rules and the use cases. Bi-lateral MOUs between the ACIC and GP&Ps will provide guidance on this area, as well as dissemination rules. Specifically, the data model below helps define rules with respect to:

- location of the stored data within the ACIC;
- ontology of the sourced FFC data sets – both population and risk indicated data;
- access to the data; and,
- archiving of the data.

Data Analytics (enriching / matching) of FFC data collections undertaken by FFC members and utilises approved analytical techniques / tools in support of FFC prioritised investigations, FFT requests for information (RFIs) and approved FFT concepts of operations (CONOPs). s 37(2)(b), s 47E(d)

[redacted]

Dissemination (reporting) of FFC data analytics undertaken by FFC members is compliant with the ACIC Act 2002 and Bi-lateral MOUs for data exchanges between the ACIC and GP&Ps. It is also reflective of GP&P legislation, administrative and compliance regimes and FFT Governance arrangements. The data model will contribute to ensuring dissemination of FFC data analytics is undertaken in a lawful and appropriate manner.

DATA REQUIREMENTS (priorities / deliverables): USE CASES

A number of different mechanisms govern the data requirements for the FFC. One of these mechanisms is a set of approved use cases. The data model will document these use cases to assist in capturing the key data requirements.

s 37(2)(b), s 47E(d)

[redacted]

Released under the Freedom of Information Act 1982 (Cth)

DATA COLLECTION (storage)

The FFC data model will provide a set of rules governing the collection (storage) of data sets sourced by the FFC. The rules will reflect the FFT Data Governance guidelines and Bi-lateral MOUs between the ACIC and TF Partners with respect to data sharing. In some instances, FFC Partners agencies and GP&Ps will agree to share data through alternate arrangements similar to that of a Bi-lateral MOUs. The data model will provide rules on the location of the stored data sets; the ontology of the data; and, access and archiving of the data.

s 37(2)(b), s 47E(d)

s 47E(d)

s 37(2)(b), s 47E(d)



DATA DISSEMINATION (reporting)

Dissemination of FFC data analysis undertaken by FFC members is compliant with the ACIC Act 2002 and any Bi-lateral MOUs for data exchanges between the ACIC and GP&Ps. Dissemination processes need also to be reflective of GP&P legislation, administrative and compliance regimes and FFC Data Governance arrangements.

There are two key elements to the dissemination process:

- the individuals who authorises the dissemination; and,
- the individual who can view the disseminated intelligence reports.

Dissemination authorisations

The majority of the dissemination will involve FFC authored reports. A portion of these reports will also include a data release in the form of FFC data sets. Occasionally, a release will just involve FFC data sets. These reports will all follow the ACIC dissemination process which requires approval by the ACIC Legal team, the ACIC Director of the FFC Intelligence team and the ACIC SES Band 1 overseeing the operations of the FFC Intelligence team.

The Bi-lateral MOUs for data exchanges might require additional dissemination rules. For example, a GP&P might require that if their data set is used in FFC authored reports, the GP&P has to be a party to the ACIC dissemination process.

Access to disseminated reports

In terms of accessing FFC reports, the broad principles regarding clearance and need-to-know apply. These reports will be appropriate caveated at, predominantly, the Official: Sensitive or Protected level. They will be clearly identified as being authored by the FFC, thereby providing guidance with respect to the need-to-know principle. The reports will be stored by the ACIC and accessing reports stored on ACIC systems will be restricted to members of the FFC.

Some reports produced by the FFC will require distribution beyond members of the FFC. The principles governing this distribution are covered in the table below.

Product type	**Recipients**
Strategic intelligence	FFC members, ACIC, AFP, all TF partner agencies
Investigative intelligence	FFC members, ACIC, AFP, investigative teams within TF partner agencies linked to the investigation
FFC data sets	FFC members, selected members of TF partner agencies with a need-to-know of FFC matters

Access to disseminated FFC data sets

The central principle of disseminating FFC data sets to GP&P is to provide:

- guidance on the prioritisation of internal administrative and compliance activities; and,
- where GP&Ps can find additional information from other agencies on individual or corporate entities who are either looking to move into their GP&P or are already operating within GP&Ps

Broadly speaking, the specifics of any risk indicator data held against and individual or corporate entity within a GP&P will not be disseminated to any other agency. The exception to this principle will only be triggered if the legislative and regulatory framework governing a GP&P and the rules covering the data exchange between the ACIC and the GP&P allow for the detailed dissemination of risk indicator data.

s 37(2)(b), s 47E(d)

Released under the Freedom of Information Act 1982 (Cth)