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.*

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

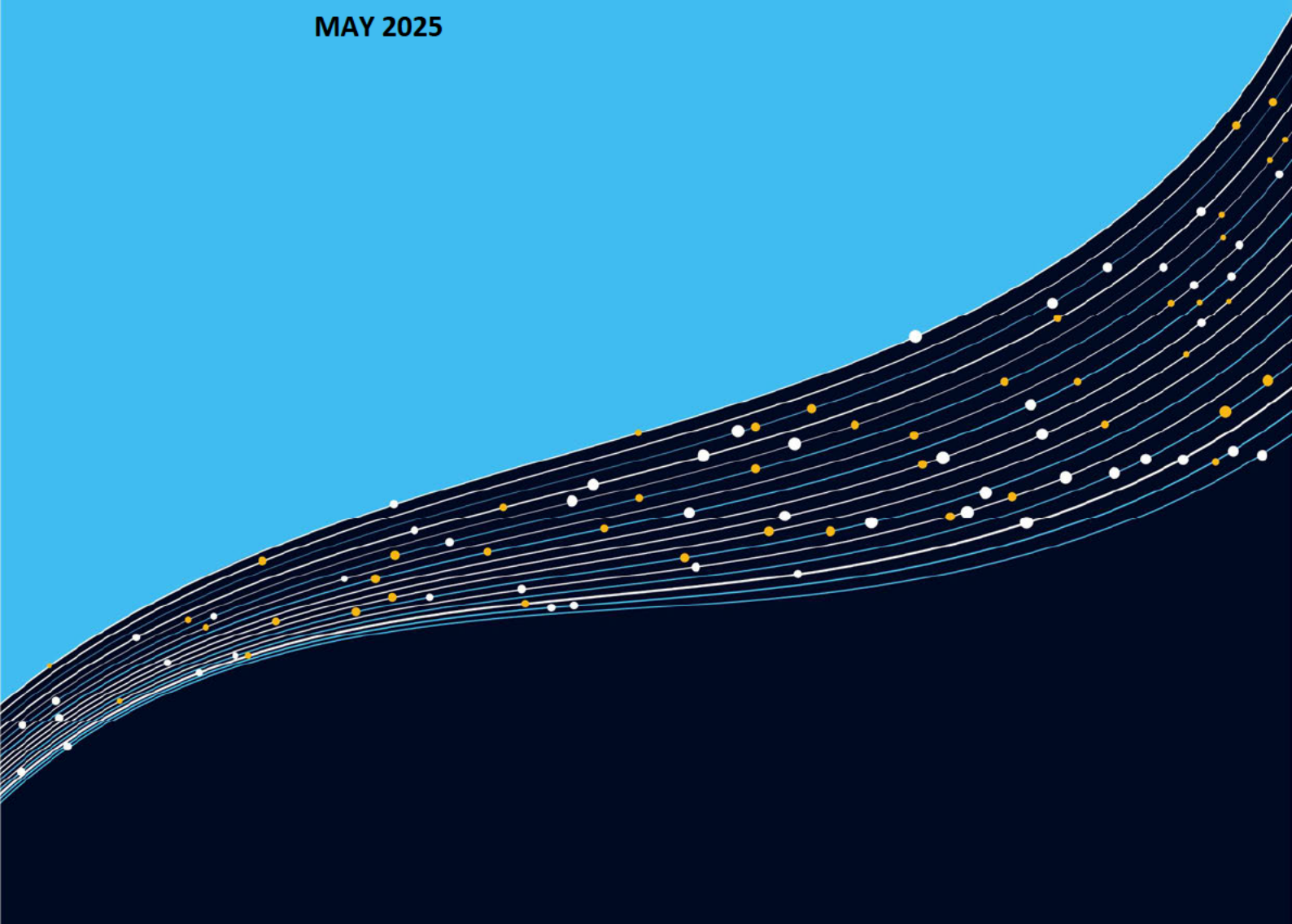
DOCUMENT 2

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

STRATEGIC ANALYSIS AND OUTREACH BRANCH

s 37(2)(b) USER GUIDE – Fraud Fusion

MAY 2025



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

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

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]

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).

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:

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.

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.

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)

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 22(1)(a)(ii)	Original Draft	Record 25/110183: Intelligence - SAO - Advanced Analytics - s 47E(d), s 37(2)(b)	1 year from approval date, or as required

DOCUMENT 3

Fraud Fusion Taskforce
Memorandum of Understanding

Dated: 25 May 2023

1. MOU Purpose and Preamble

a) This Memorandum of Understanding (MOU) commences once it is signed by a minimum of four agencies, including the NDIA and Services Australia (becoming Parties as identified in clause 3).

b) The MOU is an administrative agreement between the Parties for:

- the administration and reporting arrangements for the operating model of the Fraud Fusion Taskforce
- the provision of services and funding for the Fraud Fusion Taskforce.

c) This MOU is not intended to displace or effect legislative obligations or arrangements that the Parties might already have in place with each other or other organisations.

d) Despite the commencement date, an agency is not expected to participate (operate) under this MOU until the Accountable Authority for the agency signs the MOU on behalf of that agency.

e) The purpose of the MOU is to formalise a collaborative, productive and collegiate working relationship between the Parties, to effectively address the impact of fraud on the National Disability Insurance Scheme (NDIS) and other government support programs and payments (including related risks to participants, intended providers and other stakeholders) and to reduce the impact of fraud on the sustainability of these programs through reduction of government outlays, particularly with respect to losses from serious and organised crime (SOC – refer clause 2 for definition).

f) The Fraud Fusion Taskforce is intended to:

- facilitate the lawful, ethical and fit- for-purpose exchange of data, information, and intelligence between the Parties, particularly related to SOC exploitation of Commonwealth Government payments and programs
- support investigations and appropriate treatment of known or potential fraud; and
- inform preventative measures by the Parties or Government.

g) In establishing this MOU, the Parties agree to engage in a cooperative manner, and engage Fraud Fusion Taskforce Officers to perform activities to support:

- the provision of high-quality intelligence (under each Party's legislative framework); and
- the detection, prevention and treatment of fraud in the NDIS and other government programs and payments.

h) This MOU also outlines the roles and responsibilities of the Parties and Fraud Fusion Taskforce Officers under the agreement. It is not intended to affect the operation of legislation which may otherwise restrict the use and/or disclosure of specific information.

i) This MOU will cease upon Close of Business on 30 June 2026, unless extended by agreement of the Parties in writing in accordance with clause 13.

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)
Accountable Authority	The agency head, within the meaning given by section 7 of the *Public Service Act 1999*
ACIC	Australian Criminal Intelligence Commission, the name the Australian Crime Commission operates under as permitted by the ACC Act and the *Australian Crime Commission Regulations 2018* (Cth)
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
AFP	Australian Federal Police
AGD	Attorney-General's Department
Annexure	An annexure to this MOU
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CDPP	Commonwealth Director of Public Prosecutions
CEO	Chief Executive Officer
Close of Business	5.00PM Australian Eastern Standard Time
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
Criminal activity	Criminal activity means a criminal offence under a law of the Commonwealth, a State or a Territory of Australia
Data Governance Plan	Documented data sharing and security framework for the Fraud Fusion Taskforce
DEWR	Department of Employment & Workplace Relations
DoE	Department of Education

DoHA	Department of Health and Aged Care
DSS	Department of Social Services
DVA	Department of Veterans' Affairs
Eligible Data Breach	Has the meaning given under s26WE(2) of the *Privacy Act 1988* (Cth)
Fraud	Dishonestly obtaining a benefit, or causing a loss, by deception or other means. (Note: This is intentional action on the part of the offender)
Fraud Fusion Centre	Managed by the ACIC under an ACIC Program Head – this will operate as the centralised mechanism to enable data acquisition, detection analytics and the identification of opportunities for information-sharing. It will be staffed with Fraud Fusion Taskforce Officers from some of the Parties who will be engaged by the ACIC as ACIC members of staff under the ACC Act
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
Fraud Fusion Taskforce Officer (Taskforce Officer)	A person holding an office in, employed in or performing services for any of the Parties and engaged to work on strategic or operational activity of the Fraud Fusion Taskforce; this person is required to act to meet the purpose of the Fraud Fusion Taskforce as set out in clause 5. A Taskforce Officer for ATO disclosure purposes is defined in subsection 355-70(11) of Schedule 1 to the *Taxation Administration Act 1953* (Cth)
Fraud Fusion Taskforce Risk Management Framework	Framework setting out how the Fraud Fusion Taskforce approaches risk management and how risk management practices are integrated with governance practices, decision-making and assurance processes of the Fraud Fusion Taskforce, having appropriate regard to risk management standards and government policy
Fraud Fusion Taskforce Management Office	Teams responsible to support the Fraud Fusion Taskforce committees that provide structured governance and project management (including creation of a staged Project Management Plan), secretariat and communications functions, as well as acting as the central repository for information on projects of the Fraud Fusion Taskforce (also known as Taskforce Management Office or TMO)
Fraud Fusion Taskforce ToR	Policy document that defines the objectives, purpose and structure of the Fraud Fusion Taskforce and is endorsed by the IDC
GST	Has the same meaning as given in the *A New Tax System (Goods and Services Tax) Act 1999* (Cth)
IDC	Fraud Fusion Taskforce Inter-Departmental Committee
Loss / Waste	Taxpayer / Government money or equivalent value stolen,

	paid and/or lost due to activity not supported by the governing regulatory framework for a government program
Monitoring, Evaluation, Reporting and Improvement Framework (MERI Framework)	Overarching framework for evaluation and reporting in relation to the Fraud Fusion Taskforce that includes performance monitoring and improving the approach of the Fraud Fusion Taskforce to most effectively manage serious and organised fraud in the NDIS and other government support programs
MOU	Memorandum of Understanding
NDIA	National Disability Insurance Agency
NDIS	National Disability Insurance Scheme
NDIS Act	*National Disability Insurance Scheme Act 2013* (Cth)
NQSC	NDIS Quality & Safeguards Commission
Participant	A person who is the intended recipient of support under a government program / a related payment/s as determined by the relevant legislation and government policy (may be termed 'customer' in relation to some programs and payments)
Parties	Those agencies detailed in clause 17 of this MOU
Payment	An amount paid or payable (or the action or process of paying) to a recipient in respect of a government program that falls under the scope of the Fraud Fusion Taskforce
Payment Integrity	Ensuring payments are valid and correct in all respects, including being compliant with the legislation, paid to the appropriate person, in the correct amount and received by the intended person in a timely manner
Public Interest Certificate (PIC) – plural used: PICs	Public Interest Certificate or Authorisation – an authorisation for the disclosure of protected agency information if it meets the purposes set out in the governing legislative instrument (e.g., NDIS Act). A PIC comprehensively outlines the intended purpose of disclosure so a delegate of the CEO or other accountable authority of the agency can make an informed decision whether to disclose or not
Privacy Impact Assessment (PIA)	A systematic assessment that identifies the impact that a project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.
PSPF	Australian Government Protective Security Policy Framework, refer https://www.protectivesecurity.gov.au
Serious and organised crime (SOC)	Has the same meaning as 'serious and organised crime' given under the ACC Act
Systemic fraud	Fraud that is commonplace / widespread and is at a significant scale and risk impact to the NDIS or other government program and involves organised offending
Taskforce Integrity	Joint operation between Services Australia and the AFP to prevent, detect and disrupt serious fraud and identity crime, within the Government's system of social supports
Treatment	One or more options for addressing fraud and any related fraud risk

3. Parties

This MOU is between the agencies who agree to participate in the Fraud Fusion Taskforce and are signatories to this MOU at clause 17, as amended from time to time (Parties).

4. Status of the MOU

1) This MOU is a principles-based document setting out the overall framework within which the Parties and Fraud Fusion Taskforce Officers will work collaboratively in relation to the conduct of the Fraud Fusion Taskforce.
2) This MOU does not create legally enforceable rights and obligations between the Parties.
3) This MOU does not affect any legal rights, delegations, authorisations or obligations of a Party arising under legislation or from any other source.
4) This MOU takes precedence in relation to the administration and reporting arrangements regarding the provision of information, services and funding for the purposes of this Taskforce.
5) Where documents are created by the Fraud Fusion Taskforce Officers and Parties for the administration or governance of the Fraud Fusion Taskforce, including as required by this MOU, and where an inconsistency arises between one or more of those documents and this MOU, the terms of this MOU prevail.

5. Taskforce Purpose

Purpose

1) The purpose of the Fraud Fusion Taskforce is to improve payment integrity in government programs and payments by preventing or reducing fraud and criminal activity within and against government programs (including SOC and systemic fraud), to:
    a) protect the safety and wellbeing of participants who are at risk of harm as a result of fraud, and related service quality
    b) protect public finances and prevent or reduce financial losses
    c) ensure appropriate use of funds and the sustainability of the programs
    d) improve community confidence in the administration of those payments and programs.
2) The Fraud Fusion Taskforce will have a:
    a) Strategy focus:
        i. developing, implementing and supporting strategic preventative capability
        ii. exploring and testing options that could form the basis of future advice to Government on a scalable assurance and prevention model that could increase payment and provider integrity across government programs
        iii. well-informed cross-program actions to help prevent fraud, by drawing on the capabilities and powers of the Parties.
    b) Intelligence and operational focus:
        i. enhanced data and intelligence sharing, and intelligence development
        ii. a coordinated government approach to detection and treatment of serious and organised crime offending against government programs and systemic fraud.
3) The Fraud Fusion Taskforce will have a particular focus on the NDIS initially with broader fraud and loss detection and prevention benefits for other government programs to follow.

Taskforce Integrity will transition into the Fraud Fusion Taskforce from 1 July 2023 and be under the Fraud Fusion Taskforce remit from this date. The Fraud Fusion Taskforce will enable intelligence sharing, identification and response by the Parties to identify and address fraud perpetuated by SOC entities and others seeking to exploit the Government's programs.

Purpose statements

4) These statements are intended to support the Purpose and inform decisions on data and information sharing between Parties under the Fraud Fusion Taskforce: The Fraud Fusion Taskforce will:

   a) Identify, understand, prevent, respond to and disrupt fraud and criminal activity against the NDIS and other government programs, particularly SOC and systemic fraud, by:

      i. sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs

      ii. identifying, developing and coordinating preventative and treatment strategies domestically and internationally.

   b) Protect participant safety, service quality and the public finances of Australia, and improve payment integrity, by combatting fraud and criminal activity, including SOC and systemic fraud, against the NDIS and other government programs and payments.

   c) Enhance government coordination to prevent, detect and respond to fraud and related criminal activity within and against government programs, including SOC and systemic fraud, and improve integrity, including by:

      i. reconciling government payments to identify fraudulent transactions (such as the application of duplicate claims indicating fraudulent claims)

      ii. collecting, correlating, analysing and disseminating information and intelligence to develop appropriate responses to criminal activity and fraud, including SOC

      iii. processing new intelligence insights through multi-agency data and information sharing under the Fraud Fusion Intelligence Program, by the Fraud Fusion Centre and between the Parties and Fraud Fusion Taskforce Officers

      iv. developing capability to support a single view of entities and individuals that may be or are confirmed to be committing fraud and associated criminal activity, including SOC, in order to address associated risks

      v. enhancing and maturing the management of cases requiring active intervention, including developing different layers of case treatment and intervention.

   d) Generate and use intelligence insights to inform preventative and systemic control enhancements and further investment opportunities, drawing on the capabilities and powers of relevant agencies, including through:

      i. the identification of system vulnerabilities

      ii. cross program actions

      iii. targeted treatment to prevent fraud and criminal activity, and improve integrity in Government programs (including targeting SOC and systemic fraud).

   e) Prepare advice for Government as appropriate on a scalable assurance and prevention model that could increase payment and provider integrity across other government programs.

   Note 1: Each Party will contribute to these purposes to the extent of their legislative framework and any conditions imposed on their involvement in the Fraud Fusion Taskforce per subclause 13(4)(a).

Note 2: Terms of reference documents for the Fraud Fusion Taskforce and its committees will further outline scope, objective approach and deliverables for the Fraud Fusion Taskforce.

6. Key Principles

1) The Fraud Fusion Taskforce operates as a multi-agency Taskforce, working together to disrupt fraud and criminal activity, including SOC, and improve integrity, with the Parties recognising each other's respective roles and responsibilities in supporting their own relevant program and payment administration, intelligence, investigation and treatment processes.

2) The Parties will be operationally independent, but to the furthest extent possible, will engage in close cooperation and consultation, and ensure those employed to work on activity under the Fraud Fusion Taskforce (Taskforce Officers), achieve efficient and effective outcomes from both an individual agency and across government perspective in accordance with the Fraud Fusion Taskforce purpose clause 5.

3) The Fraud Fusion Taskforce will uphold the safety, security and wellbeing of participants of the NDIS and customers of other government programs and payments as its highest priority. The Fraud Fusion Taskforce will have primary regard to any risks arising for participants and customers when considering relevant and appropriate treatment options for matters in relation to alleged or confirmed fraud.

4) The Fraud Fusion Taskforce will be underpinned by a rigorous Ethics & Human Oversight Framework, to be endorsed by the IDC, and will have human oversight of all decision logic, governance controls and treatment approaches determined by the Fraud Fusion Taskforce.

7. Governance and Responsibilities

1) NDIA and Services Australia will jointly lead the Fraud Fusion Taskforce and will work together with all Parties to manage the overall performance of the Fraud Fusion Taskforce.

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.

3) A Fraud Fusion Taskforce Inter-Departmental Committee (IDC) will be co-chaired by Deputy CEOs of the NDIA and Services Australia (i.e., Senior Executive Service (SES) Band 3 members). The IDC will:

   a) Operate under its own terms of reference.

   b) Have a membership of other representatives at SES Band 2 or above from NDIA, Services Australia, ACIC, AFP, AGD, ATO and NQSC, which will be responsible for:

      i. providing strategic oversight and monitoring of the effective and efficient operation of the Fraud Fusion Taskforce and its performance against the deliverables

      ii. overseeing and guiding other Taskforce committees (refer subclauses 7(4) and 7(6)) and providing advice to the Parties and Fraud Fusion Taskforce Officers in pursuit of the Fraud Fusion Taskforce objectives and deliverables, to meet the Purpose in clause 5.

4) For the IDC, proxy representation is allowed at SES Band 2 or above, or by exception below SES Band 2 with the agreement of both Co-Chairs. The Co-Chairs can be proxy for each other; or if neither is available, they can assign a proxy of their choice.

5) A Strategic Prevention Committee (SPC) will be chaired by SES Band 2 or above from one or more of the Parties and will comprise suitably skilled and experienced Fraud Fusion

Taskforce Officers at SES Band 1 or above from the Parties. The SPC will:

a) Operate under its own terms of reference.

b) Be responsible for developing, implementing and supporting strategic preventative capability; and exploring and testing options that could form the basis of future advice to Government on a scalable assurance and prevention model that could increase payment and provider integrity across government programs.

6) For the SPC, proxy representation is allowed at Executive Level 2 (EL2) or above. The Co-Chairs can be proxy for each other; or they can assign a proxy of their choice.

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:

a) Operate under its own Terms of Reference, and in accordance with the functions and powers afforded to ACIC in the *Australian Crime Commission Act 2002* (Cth) (ACC Act).

b) Be comprised of members of the staff of the ACIC as defined in section 4 of the ACC Act, some of whom may be Fraud Fusion Taskforce officers substantively employed by Parties other than the ACIC (where agreed with these other Parties), and who are engaged by the ACIC for delivery of the Fraud Fusion Intelligence Program (including the Fraud Fusion Centre).

c) Some ACIC staff involved in the delivery of the Fraud Fusion Intelligence Program are provided for in funding under the October 2022 budget measure, *Fraud Fusion Taskforce*.

d) Oversee the activities of the Fraud Fusion Centre, including its administration, intelligence development, and data sharing.

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

f) Receive and consider requests for information from the IOC and the Parties for the purposes of the Taskforce.

g) Provide, as permitted by the ACC Act and relevant ACIC policies, intelligence products to the IOC and the Parties for the purposes of the Taskforce.

8) An Intelligence and Operations Committee (IOC) will be chaired by Fraud Fusion Taskforce Officers at SES Band 2 or above from one or more of the Parties and will comprise of suitably skilled and experienced Fraud Fusion Taskforce Officers at SES Band 1 or above from the Parties. Members can assign a proxy at EL2 or above. Co-Chairs can proxy for each other or can assign a proxy of their choice. The IOC will:

a) Operate under its own terms of reference.

b) Have responsibility for overseeing all Taskforce intelligence matters and activities of the Fraud Fusion Taskforce. The Fraud Fusion Centre will be established, operated and led by the ACIC, resourced as outlined in subclause 7-7(b) and (c). The Program Head for the Fraud Fusion Intelligence Program and the Fraud Fusion Centre will attend, and engage with, the IOC.

c) Guide intelligence development, data sharing and use concepts and contribute to the Fraud Fusion Taskforce's evaluation of its performance in generating and using intelligence in pursuit of the Fraud Fusion Taskforce's objectives.

d) Be responsible for overseeing and deliberating on Taskforce operations and activities including deployment of resources to achieve the Fraud Fusion Taskforce's purpose.

e) Ensure a focus on strategic insights and case level treatments informed by coordinated intelligence and using data analysis capabilities. This is to support the effective and appropriate treatment of fraud and associated criminal activity, including SOC and systemic fraud, in relation to the NDIS and other government programs, and

improve integrity.

f) Ensure the smooth and seamless transition of the existing Taskforce Integrity into this Taskforce commencing 1 July 2023. This process will be facilitated and supported by a transition plan developed by Services Australia and endorsed by the IDC.

g) Act as the point of escalation and decision for matters where:

i. a multi-agency response has been determined to be required, or alternative treatment options are required for timely and effective resolution of fraud matters; or

ii. there are other matters of significance which might affect or impact the effective operations and delivery of the Fraud Fusion Taskforce.

Note: Requests will be made of the ACIC Fraud Fusion Intelligence Program Head and ACIC with respect to the Fraud Fusion Intelligence Program and Fraud Fusion Centre as part of the arrangements for the Fraud Fusion Taskforce. These requests, which may be termed 'guidance', do not constitute or take the form of direction of the ACIC or its officers, including in relation to performance of the ACIC's functions or exercise of its powers; there is no oversight of the ACIC by the Fraud Fusion Taskforce committees or other Parties to the Fraud Fusion Taskforce.

9) The Fraud Fusion Taskforce Management Office (TMO), resourced by the NDIA, will be responsible for governance and coordinating reporting responsibilities under the Fraud Fusion Taskforce including but not limited to:

a) Setting the governance and reporting arrangements for the Fraud Fusion Taskforce.

b) Administering the Secretariat for the Fraud Fusion Taskforce committees (which is part of the TMO).

c) Coordinating the review of this MOU (and terms of reference for the aforementioned committees).

d) Monitoring and leading the overall program management and performance of the Fraud Fusion Taskforce.

e) Establishing and maintaining the Fraud Fusion Taskforce Communication and Engagement Strategy.

f) Developing and monitoring a Taskforce evaluations framework (MERI Framework).

10) In addition to (or under) the TMO, other functions and roles may be established as needed to support the delivery of the Fraud Fusion Taskforce.

11) Subject to subclause 7(2), the Parties will:

a) Actively assist each other, engage Fraud Fusion Taskforce Officers, and collaborate to meet the Fraud Fusion Taskforce's purpose (outlined in clause 5) and address the strategic framework endorsed by the IDC as set out in the Fraud Fusion Taskforce ToR with adherence to the key principles identified in clause 6.

b) Provide, at a minimum, resources and effort consistent with the Commonwealth's October 2022 Budget measure *Fraud Fusion Taskforce* – refer to the Fraud Fusion Taskforce ToR and any other allocated Taskforce funding.

c) Report on all activities undertaken and resources used to support the Fraud Fusion Taskforce under the arrangements referred to in this MOU and report to the co-lead agencies, NDIA and Services Australia, and the TMO and Taskforce committees, as required.

d) Make operational and intelligence capabilities available to the Fraud Fusion Taskforce (subject to the note below), within available resources and consistent with relevant laws, to improve integrity and maximise opportunities to proactively detect, prevent and respond to fraud and associated criminal activity, particularly SOC, against the NDIS and other government programs and payments.

Note: ACIC will direct the Fraud Fusion Centre to make its capabilities available to

align with the Fraud Fusion Taskforce Intelligence Program's purpose (subclause 7(7)) and objectives, as permitted by ACIC's legal framework.

e) Be responsive and engage early with other Parties on new matters of relevance to the Fraud Fusion Taskforce including requests for variation of services agreed under this MOU, the Fraud Fusion Taskforce ToR, or to develop, cost and expand on existing or new initiatives.

12) Each Party will perform the services as outlined for the specific agency in **Annexure A**. In respect of this, each Party acknowledges that **Annexure A** should not be interpreted as restricting involvement or participation of each Party but an overview of the specialist capabilities to the Fraud Fusion Taskforce.

13) See **Annexure B** for a diagrammatic representation of the high-level Taskforce governance.

8. Communication

1) Subject to subclause 8(2) below, the Parties undertake not to release any public statement or media in relation to the Fraud Fusion Taskforce, any Taskforce operations or this arrangement, without consulting the IDC Co-Chairs, or staff appointed for such purposes, who will liaise with the relevant media officers of the Parties involved.

2) Subclause 8(1) is not intended to restrict the Parties from complying with their communications obligations in respect of applicable governing legislation.

3) A Taskforce Communication and Engagement Strategy, endorsed by the IDC, shall be maintained by the TMO and available for all Parties to apply in a coordinated manner. The Parties agree to comply with this Strategy subject to their respective obligations and powers under legislation.

4) Except where there is an express legal or legislative constraint, each of the Parties agrees to consult affected IDC members, and the IDC Co-Chairs (or their nominated delegates) on any request or order for access or disclosure relating to the Fraud Fusion Taskforce or its business that is made to them under the *Privacy Act 1988* (Cth) (Privacy Act), *Freedom of Information Act 1982* (Cth) or legal proceedings regarding the Fraud Fusion Taskforce. This excludes normal investigations and prosecution business of the Fraud Fusion Taskforce that will be reported on a regular basis as set out in the MERI Framework.

Note: subclause 8(3) is not intended to replace existing FOI processes that may also occur between Commonwealth agencies and could occur in parallel.

9. Evaluation, Reporting, Asset and Risk Management

1) A MERI Framework and a Taskforce Risk Management Framework will be developed under direction of the IDC for endorsement by the IDC and implementation by the Parties.

2) Subject to subclauses 9(3)-(6):

a) Intellectual property and other assets/items used for the Fraud Fusion Taskforce vests in each of the Parties respectively. This includes background intellectual property created prior to the establishment of the Fraud Fusion Taskforce which shall remain the property of the agency that created it.

b) Where use of intellectual property is necessary for the performance of the Fraud Fusion Taskforce, Parties undertaking the relevant nominated activities under the Fraud Fusion Taskforce have a non-exclusive, royalty-free license to use the intellectual property of other Parties.

3) Custody arrangements for intellectual property and other items/assets may be agreed between agencies from time to time based on determination of the owner agency, in order to undertake the activities of the Fraud Fusion Taskforce in an effective and appropriate

manner.

4) New intellectual property created by the Fraud Fusion Taskforce will vest in the agency determined by the IDC and will be used by other agencies, where legally, permissible, for the purpose of the Fraud Fusion Taskforce pursuant to any agreements between two or more Parties in the Fraud Fusion Taskforce, including the Fraud Fusion Taskforce Data Governance Plan and Intelligence agreements.

5) Each of the Parties warrants that use of any intellectual property will not infringe the intellectual property rights of any third party.

6) Intellectual property contributed for use under the Fraud Fusion Taskforce, and as described in this clause 9, survives termination of this MOU.

10. Work Health and Safety and Location

1) Each of the Parties agree to take all reasonable steps to provide a safe working environment, which does not pose avoidable health or physical safety risks for Fraud Fusion Taskforce Officers. This will include Agency specific induction and orientation (i.e., managed by each of the Parties).

2) Fraud Fusion Taskforce Officers of the Parties will work at their own secure work and office locations, except where engaged to work in other Party offices, including the Fraud Fusion Centre in ACIC offices.

11. Legal and Ethical Issues

1) The Parties undertake to inform the IDC Co-Chairs or their delegates of any legal or ethical issues or potential issues that may impact the effectiveness or reputation of the Fraud Fusion Taskforce or another Party/ies in relation to the Fraud Fusion Taskforce. The Parties will cooperate in the management of any legal or ethical issues that relate to the Fraud Fusion Taskforce and manage these through appropriate channels.

2) Each of the Parties acknowledges they will appropriately obtain legal advice, relevant to their statutory responsibilities and support programs, and implement effective controls to mitigate the potential for incidents that may result in legal proceedings or other ethical matters that could impact the standing of the Fraud Fusion Taskforce or other Parties.

12. Dispute Resolution

1) The Parties agree that any dispute concerning this MOU should be resolved in the spirit of good faith and open communications.

2) The Parties must attempt to resolve any dispute concerning this MOU by presenting the matter under dispute to the IDC Co-Chairs in the first instance.

3) In the event a dispute is escalated to the IDC Co-Chairs, the Parties involved shall be consulted, with any proposed resolution negotiated between the Parties and approved by one or both IDC Co-Chairs.

4) Where the IDC Co-Chairs and the Parties involved fail to reach a satisfactory resolution within 30 days of the dispute being raised, the matter shall be escalated to the IDC (full committee) for consideration and action as appropriate.

5) Each Party will bear their own costs in complying with this clause 12 and will, to the extent possible, continue to perform operations under this MOU pending resolution of the dispute.

6) In the event of a dispute between the Fraud Fusion Taskforce committees, the decision of the IDC takes precedence.

7) Matters in dispute, for resolution under subclauses 12(1) to 12(6), do not include matters

arising from ACIC decision-making in respect of the Fraud Fusion Intelligence Program; this relevantly includes ACIC decisions made to ensure compliance with the ACC Act and other enabling or relevant legislation. Should there be a dispute as to how ACC information may be used, or how the Fraud Fusion Intelligence Program is to be conducted, the ACIC is able to exercise a veto vote (such that it can comply with its own legislative framework).

13. Commencement, Duration, Variation and Termination

1) **Commencement**

   a) This MOU commences on the date that NDIA and Services Australia and two other agencies have signed the MOU, acknowledging that the date the MOU is signed by each of the other Parties may post-date commencement.

   b) The Parties are not expected to operate under this MOU until they sign this MOU.

2) **Duration**

   a) Consistent with the Fraud Fusion Taskforce October 2022 Budget measure announcement, it is intended this MOU will remain in force until 30 June 2026, subject to subclause 13(5).

   b) The IDC shall review this MOU no later than six months prior to expiry of the MOU. Upon review, this MOU may be extended in accordance with subclause 13(5). Agreement to extend may be subject to further funding being allocated to the Fraud Fusion Taskforce through future Budget processes.

3) **Variation and Review**

   a) This MOU may be varied by agreement of all the Parties in writing. Any variation or modification must be aligned to the intent of the relevant Budget measure/s and Fraud Fusion Taskforce purposes.

   b) The TMO will be responsible for consulting on and drafting any variations or amendments to this MOU, to be endorsed by the IDC.

   c) An annual review of the MOU will be conducted by the IDC, coordinated by the TMO.

4) **Variation of the Parties**

   a) The IDC will consult with all Parties to the MOU prior to any variation to the MOU to include a new Party.

   b) The IDC may establish separate conditions that will apply to the new Party to the MOU, having regard to the statutory functions and intended contribution of the new Party to the Fraud Fusion Taskforce.

   c) All Parties to the MOU acknowledge and agree that the IDC Co-Chair may execute the New Party Addendum in **Annexure C** on behalf of all Parties to the MOU to include the new Party to the Fraud Fusion Taskforce and the MOU and to vary the MOU to establish any separate conditions that will apply to the new Party.

   d) The TMO will be responsible for administering the inclusion of any new Party to the Fraud Fusion Taskforce and this MOU and execution by the new Party of the New Party Addendum in **Annexure C**.

5) **Termination**

   a) This MOU will remain in force until 30 June 2026, as outlined in subclause 13(2), unless a decision is taken in writing by the IDC to extend the duration of the MOU or the MOU is terminated earlier by agreement in writing of the IDC.

   b) Where an individual Party wishes to withdraw from the MOU, they may do so by sending a notice of termination in writing to the IDC Co-Chairs. The Parties agree that any withdrawal is to be managed in the spirit of cooperation and to minimise adverse

impact to the work of the Fraud Fusion Taskforce.

c) Termination by one or more agencies that were party to the Fraud Fusion Taskforce and this MOU does not affect the continued operation of this MOU between the remaining Parties.

d) A Party intending to terminate should provide 30 days' notice of termination or such other period as agreed with the IDC Co-Chairs and take all reasonable steps prior to termination to ensure the intent of the budget measure/s remains achievable for the remaining Parties.

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.

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

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].

4) To ensure adherence to the disclosure rules in the *Taxation Administration Act 1953* (Cth), the ATO has developed an ATO Data & Intelligence Disclosure Governance Plan which outlines the legislative framework, governance, data stewardship, ATO intelligence collection methodology and disclosure process, which provides the framework for disclosure of ATO protected information to the Fraud Fusion Taskforce.

5) Upon becoming a party to this MOU, each respective agency also agrees to adhere to the ATO Data & Intelligence Disclosure Governance Plan to exercise good data stewardship and ensure the lawful, ethical and fit for purpose disclosure and use of ATO protected information.

16. GST

1) GST will be separately managed by each of the Parties in respect of their own receipt of funding and delivery of the services under the Fraud Fusion Taskforce.

2) GST will not apply to the funding amounts outlined in the services at **Annexure A**. See Note below. For all other amounts that may become payable under this MOU and are not specifically in respect of services in **Annexure A**, each Party must provide to the other all information reasonably required to determine whether the supply is subject to GST.

Note: GST is generally imposed on supplies made for consideration. However, certain payments made by one government related entity to another are not taken to be the provision of consideration – see section 9-17 of the *A New Tax System (Goods and Services Tax) Act 1999* (Cth).

---

[1] Subdivision 355-B of Schedule 1 to the *Taxation Administration Act 1953* (Cth)
[2] A Taskforce Officer *(taskforce officer)* for ATO disclosure purposes is defined in subsection 355-70(11) of Schedule 1 to the *Taxation Administration Act 1953* (Cth)
[3] Subsection 355-70(1) table item 4 of Schedule 1 to the *Taxation Administration Act 1953* (Cth)
[4] Section 355-30 of Schedule 1 to the *Taxation Administration Act 1953* (Cth)

17. Signatories

.....
NDIA
..... day 2023

.....
Services Australia
..... day 2023

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

.....
ACIC
21st day June 2023

.....
AGD
..... day 2023

.....
NQSC
..... day 2023

.....
AFP
..... day 2023

.....
ATO
..... day 2023

.....
CDPP
..... day 2023

.....
DSS
..... day 2023

.....
AUSTRAC
..... day 2023

.....
ASIC
..... day 2023

.....
DEWR
..... day.....2023

.....
DoHA
..... day 2023

.....
DoE
..... day.....2023

.....
DVA
..... day 2023

.....
..... day.....2023

Annexure A

Delivery of services by Parties to the MOU

In delivering Fraud Fusion Taskforce services, the participating agencies that agree to be Parties will work closely with each other and report on activities to appropriate governance bodies of the Fraud Fusion Taskforce and the TMO as required The agencies and their services are

NDIA

ABN 25 617 475 104

The National Disability Insurance Agency (NDIA) is the co-lead agency for the Fraud Fusion Taskforce It will provide data and analytics support to the Fraud Fusion Taskforce through a resource contribution to the ACIC led Intelligence program, access to relevant databases and support for appropriate data interface and analysis NDIA will also progress existing and new cases operationally and develop longer term systemic controls to reduce fraud and loss to the NDIS It will provide coordination support for the Fraud Fusion Taskforce

Primary responsibilities

- Co-Lead for the Fraud Fusion Taskforce
- Contribution of outposted resourcing to ACIC led Intelligence program
- Internal support for data sharing and analysis
- Operational resourcing to pursue existing and new cases of fraud
- Provide coordination support for oversight, governance, reporting and communication for the Fraud Fusion Taskforce

Services Australia

ABN 25 617 475 104

Services Australia will co-lead the Fraud Fusion Taskforce and collaborate with the Fraud Fusion Taskforce through sharing of information relevant to Taskforce activities and operations to help better identify and deal with sophisticated criminal networks The collaboration will assist with the identification and management of scams, crime affecting the administration of MyGov, Commonwealth payment fraud and associated links to serious and organised crime entities Services Australia will oversee the transition of Taskforce Integrity into the Fraud Fusion Taskforce during 2023-24

Primary responsibilities

- Co-Lead for the Fraud Fusion Taskforce
- Contribution of resourcing seconded to ACIC led Intelligence program
- Internal support for data sharing and analysis
- 2023-24 operational resourcing to take appropriate action arising from Taskforce Integrity as part of its transition to the Fraud Fusion Taskforce
- Provision of Forensic Services capability (to be progressively built over time)

ACIC

ABN 11 259 448 410

The Fraud Fusion Taskforce Intelligence Program will be led by the Australian Criminal Intelligence Commission (ACIC) and will involve the ACIC linking and using 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 The 'Fraud Fusion Centre' will be established by ACIC and used as the mechanism to enable enhanced data acquisition, detection analytics and sharing co-located at the ACIC

Primary responsibilities

- Lead for the Fraud Fusion Taskforce Intelligence Program
- Responsible for establishment and management of the Fraud Fusion Centre and will contribute expert resource to it
- Data Governance and assurance
- Data acquisition, storage and detection analytics
- Delivery of strategic, operational and tactical intelligence products and insight

NQSC

ABN 40 293 545 182

The NDIS Quality and Safeguards Commission (NQSC), as the regulator for the National Disability Insurance Scheme (NDIS), plays a key role in investigating and taking compliance action against providers and workers who have been identified as not complying with provisions in the NDIS Act including where they may have committed fraud or contributed to the abuse and exploitation of NDIS participants It will also provide data and analytics support to the Fraud Fusion Taskforce through a resource contribution to the ACIC led Intelligence program and access to relevant databases and support for appropriate data interface and analysis

Primary responsibilities

- Contribution of outposted resourcing to ACIC led Intelligence program
- Internal support for data sharing and analysis
- Operational resourcing to take appropriate compliance action against providers and workers

AGD

ABN 92 661 124 436

The Attorney-General's Department (AGD) provides Whole-of-Government policy advice on fraud, loss and prevention in the Commonwealth AGD also manages extradition and mutual assistance requests for formal assistance to and from other jurisdictions in relation to criminal investigations and prosecutions AGD also contributes to the development of advice to Government, including policy, insights and measured benefits

Primary responsibilities

- Whole-of-Government policy advice on fraud and loss within current functions

AFP

ABN 17 864 931 143

The Australian Federal Police (AFP) will provide the Fraud Fusion Taskforce both criminal and civil treatment options The AFP conducts criminal investigations into serious crime in line with endorsed concepts of operations Any other criminal matters that may be identified as a result of the initial investigation may be separately referred to the AFP AFP produces intelligence and engages in proceeds of crime forfeitures and litigation The AFP will support the Fraud Fusion Taskforce through the placement of senior investigators into leadership roles in Taskforce triage and assessment, which will translate intelligence into proactive and coordinated treatment and response activities across a spectrum of civil, criminal, administrative and regulatory actions These senior officers will also support NDIA and other agency criminal investigations by providing guidance and assistance to investigators to develop, improve and achieve successful results, and to guide, coach and mentor investigators, aiming to improve consistency and standards The AFP will also embed intelligence officers into the ACIC led Fraud Fusion Intelligence cell

Outside of the Fraud Fusion Taskforce, the AFP has a range of key operational capabilities and services, which it prioritises towards the highest criminal threats and risks, such as complementary or concurrent criminal investigations, international coordination and support, and covert intelligence collection capabilities The AFP will continue to utilise these base-funded capabilities and services to support the Fraud Fusion Taskforce on a referral basis, in accordance with the AFP operational prioritisation model

Primary responsibilities

- Contribution of senior investigators into Taskforce triage and assessment
- Contribution of outposted resourcing to ACIC led Intelligence program
- Operational support for criminal action against those committing fraud, including investigation lead and support, criminal asset confiscation and law enforcement liaison
- 2023-24 operational resourcing to continue Taskforce Integrity as it transitions into the Fraud Fusion Taskforce

ATO

ABN 51 824 753 556

The ATO will provide

- Analytics resourcing and support for deliverables such as pattern detection that improve insights into potential fraud occurring across the agreed Fraud Fusion Taskforce priority programs and focus areas, including in the Fraud Fusion Centre
- Appropriate sharing and guided use of ATO data within the Fraud Fusion Centre
- Tactical and operational intelligence support in response to Fraud Fusion Taskforce requests to the ATO for information relevant to suspected fraudulent claims, and
- Strategic intelligence support through the use of ATO data analysts and intelligence officers conducting work to support the broader Taskforce Intelligence Program, including the identification of fraud networks across payment programs

Primary responsibilities

- Contribution of outposted resourcing to the ACIC led Intelligence program, including the Fraud Fusion Centre
- Contribute to the operational activities of the Fraud Fusion Taskforce, including appropriate data sharing and analysis, drawing on the ATO's extensive data and intelligence capabilities
- Contribute to the strategy and prevention activities of the Fraud Fusion Taskforce, including the deliverables of the Strategic Prevention Committee

CDPP

ABN 41 036 606 436

The Commonwealth Director of Public Prosecutions (CDPP) will provide pre-brief advice to ensure that investigations are conducted as efficiently and effectively as possible, provide mutual assistance and extradition-related services, assess and prosecute appropriate matters through the courts, and conduct (in appropriate cases) conviction-based proceeds of crime applications Serious crime referrals are amongst the most complex and resource intensive prosecutions conducted by the CDPP

Primary responsibilities

- Supporting legal advice and action to address and progress criminal cases

ASIC

ABN 86 768 265 615

The Australian Securities & Investments Commission (ASIC) has the power to investigate matters where it has reason to suspect a contravention of the *Corporations Act 2001* (Cth) ASIC may take its own enforcement or regulatory actions (administrative or civil action, or criminal briefs to the CDPP) regarding such contraventions, which could include a failure to comply with directors'/other company officers' duties in respect of illegal phoenix activity, market misconduct and financial services contraventions, among other matters

Primary responsibilities

- Contribution of outposted resourcing to ACIC led Intelligence program
- Operational support to investigate and take action against fraud within its powers

AUSTRAC

ABN 32 770 513 371

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is responsible for detecting, deterring and disrupting criminal abuse of the financial system to protect the community from serious and organised crime The Fraud Fusion Taskforce will leverage AUSTRAC's intelligence, data analytics and regulatory capabilities and expanding international network to detect and dismantle new threats targeting Australian government systems This will occur through the development and dissemination of AUSTRAC intelligence products, intelligence collaboration and the consideration of regulatory responses where appropriate AUSTRAC will collaborate with the financial sector through the Fintel Alliance to facilitate the identification and analysis of unknown entities and individuals engaged in serious financial crime whilst also expanding the financial profile of known entities

Primary responsibilities

- Contribution of outposted resourcing to ACIC led Intelligence program
- General intelligence and analytics advice and support within current functions

DoHA

ABN 83 605 426 759

As a Party, the Department of Health and Aged Care (DoHA) will provide data and analytics support to the Fraud Fusion Taskforce through a resource contribution to the ACIC led Intelligence program, access to relevant databases and support for appropriate data interface and analysis

Primary responsibilities

- Contribution of outposted resourcing to ACIC led Intelligence program
- Internal support for data sharing and analysis

DVA

ABN 23 964 290 824

The Department of Veterans' Affairs (DVA) will provide data and analytics support to the Fraud Fusion Taskforce through a resource contribution to the ACIC led Intelligence program, access to relevant databases and support for appropriate data interface and analysis

Primary responsibilities

- Contribution of outposted resourcing to ACIC led Intelligence program
- Internal support for data sharing and analysis

DoE

ABN 12 862 898 150

The Department of Education (DoE) will provide data and analytics support to the Fraud Fusion Taskforce through a resource contribution to the ACIC led Intelligence program, access to relevant databases and support for appropriate data interface and analysis

Primary responsibilities

- Contribution of outposted resourcing to ACIC led Intelligence program
- Internal support for data sharing and analysis

DEWR

ABN 96 584 957 427

The Department of Employment and Workplace Relations (DEWR) will provide data and analytics support to the Fraud Fusion Taskforce through a resource contribution to the ACIC led Intelligence program, access to relevant databases and support for appropriate data interface and analysis

Primary responsibilities

- Contribution of outposted resourcing to ACIC led Intelligence program
- Internal support for data sharing and analysis

DSS

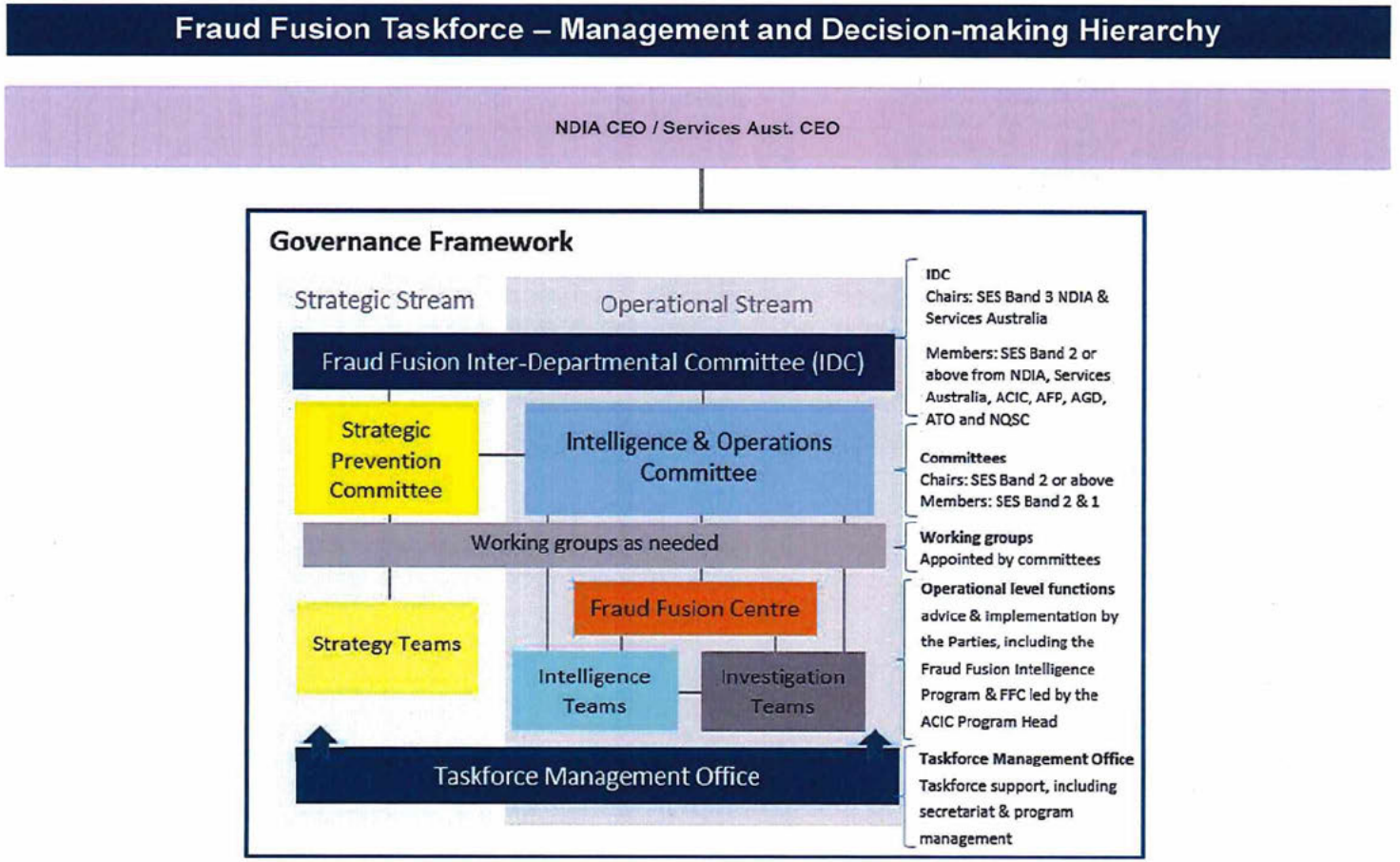
ABN 36 342 015 855

The Department of Social Services (DSS) has policy responsibility for social security payments related to Taskforce Integrity (Taskforce Integrity will come under the remit of the Fraud Fusion Taskforce from 1 July 2023) and is the portfolio department for the Fraud Fusion Taskforce lead agencies, NDIA and Services Australia

Annexure B

Governance diagram

This diagram is for illustrative purposes only. Please note that this diagram does not extend to specifically identify any working groups established to support the operationalisation of the Fraud Fusion Taskforce that may report from time to time to the committees, Co-Lead agencies, NDIA and Services Australia, and/or the ACIC Program Head as relevant under the terms of the MOU.



Annexure C

Fraud Fusion Taskforce New Party Addendum – to become a Party to the Fraud Fusion Taskforce and Memorandum of Understanding (MOU)

Between: _____("the New Party") and the other Parties to the Fraud Fusion Taskforce and MOU.

Effective date: _____

1. The New Party wishes to become a Party to the Fraud Fusion Taskforce and the MOU.
2. The existing Parties to the Fraud Fusion Taskforce and MOU wish to accept the New Party as one of the Parties, subject to the following conditions (to be included in services to be performed in variation to Annexure A to the MOU):

   (Insert relevant conditions)
3. A Fraud Fusion Taskforce IDC Co-Chair, on behalf of the existing Parties, accepts the New Party to the Fraud Fusion Taskforce and MOU, subject to the terms of the MOU (including any subsequent amendments thereto) and any conditions in this Addendum, as of the above stated effective date.

New Party:

Signed on behalf of the New Party (the Agency) by the intended SES Band 3 representative:

_____

_____
(Name and Title of New Party i.e., applying

Agency Representative)

Date: _____

Existing Parties:

Signed on behalf of the IDC and existing Taskforce Parties by the Fraud Fusion Taskforce IDC Co-Chair:

_____

_____
(Name and Title of Fraud Fusion Taskforce IDC Co-Chair)

Date _____

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Fraud Fusion Taskforce

OFFICIAL

Taskforce Intelligence Program – Operating Model

Context

The Fraud Fusion Taskforce (hereafter "the Taskforce") commenced on 1 November 2022. The Taskforce is co-led by the National Disability Insurance Agency (NDIA) and Services Australia (SA) and supersedes the NDIS Fraud Taskforce and Taskforce Integrity.

Taskforce Objectives

The Taskforce seeks to cause systemic change within the ecosystem surrounding Commonwealth payments and programs to minimise fraud, mitigate risks for users of such payments and programs and ensure that Commonwealth monies are spent for the legitimate benefit of such users.

The Taskforce will achieve systemic change on a continuum from tactical to strategic through supporting the following outcomes:

(1) Fraud Deterrence (through criminal prosecution outcomes and alternative disruption, including administrative action – to be referred to collectively as "treatment outcomes" - and a communications plan)

(2) Enhanced Risk Identification and Mitigation

(3) Policy Change and Legislative Reform

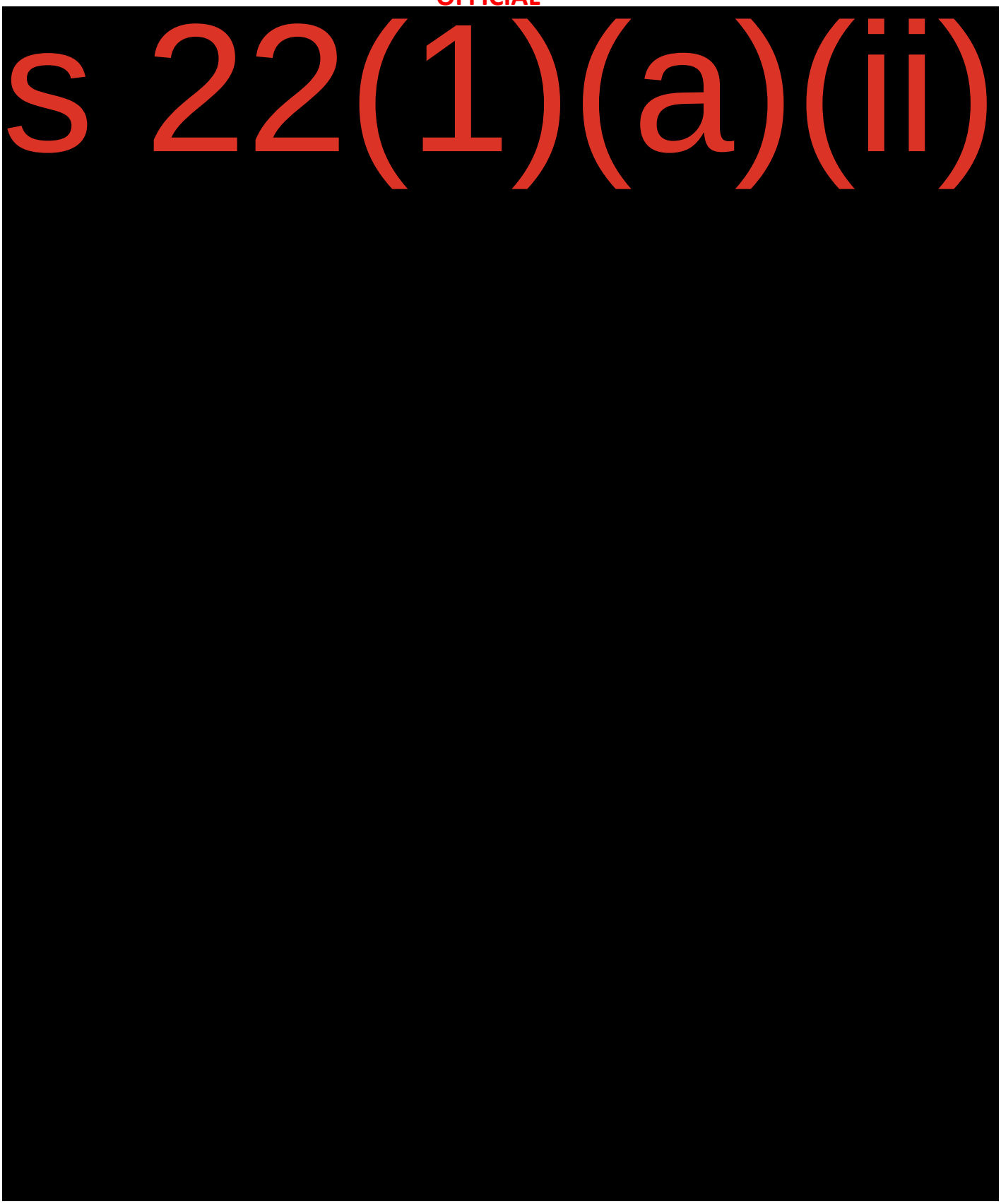
It is anticipated that the systemic change will result in large-scale, measurable savings to the taxpayer and enhanced outcomes for users of Government payments and programs.

Taskforce Intelligence Program

The Taskforce Intelligence Program (TIP) is the centrepiece of the Taskforce, providing the intelligence base to support Outcomes (1) – (3). The ACIC National Manager Operational Strategy (NMOS) will lead the TIP in collaboration with Taskforce partners and will be a key member of the SES1-level Taskforce Intelligence and Operations Committee.

At the heart of the TIP will be the Fraud Fusion Centre, which will be physically located in the ACIC. The Fraud Fusion Centre will be supported by intelligence teams located in each Taskforce agency, with those teams becoming part of the TIP to the extent that they are working on Taskforce matters. It is important to note that all agencies are operationally independent but will collaborate on priorities determined by the Executive leadership of Taskforce participant agencies.

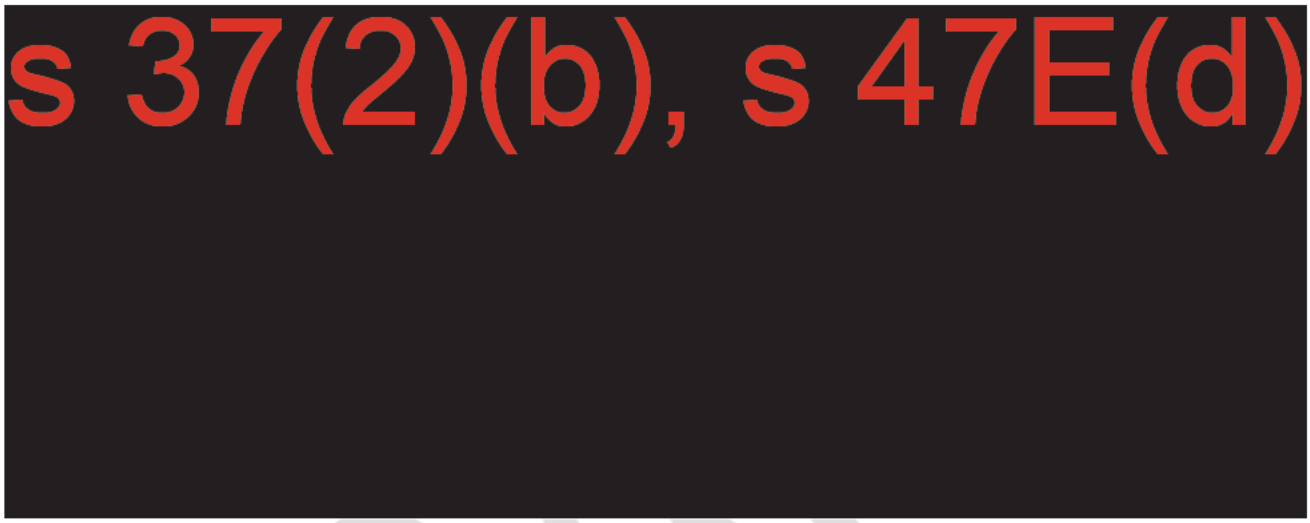
The work of the Fraud Fusion Centre will be led and directed by the Director Fraud Fusion Centre, who is the Senior Responsible Officer for ACIC Project Minoru pursuant to the *Special ACIC*


s 22(1)(a)(ii)

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.



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.

- 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)

Fraud Fusion Centre Collection Plan

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Title

Fraud Fusion Centre (FFC)

Background

In October 2022, the Government committed $126.3 million over four years to establish the Fraud Fusion Taskforce (FFT), with an aim to reducing the incidents and opportunity for non-compliance and existing or emerging serious and organised crime (SOC) exploitation of the National Disability Insurance Scheme (NDIS) and other Government payments and programs.

The purpose of the FFT is to improve payment integrity in Government programs by preventing or reducing SOC exploitation.

The Intelligence and Operational focus of the FFT is enhanced intelligence and data-sharing, and a whole of government, coordinated approach to detection and treatment of SOC exploitation and systemic fraud of government programs.

The Australian Criminal Intelligence Commission (ACIC) leads the Fraud Fusion Centre (FFC), consisting of representatives from the ACIC and some FFT member agencies. The FFC operates as the primary mechanism to enable data acquisition, detection analytics, and intelligence generation and sharing between participating FFT agencies in the FFC. The FFC will be staffed as a multi-disciplinary team, consisting of Analysts, Investigators, Data Scientists, fraud and compliance subject matter experts, and possibly Financial Investigators.

Collection capabilities that will be used include, but are not limited to:

- Bulk data analytics
- Data-matching across participating agency database information
- ACIC coercive powers
- Human source
- Strategic Intelligence

From the ACIC perspective, collection activities conducted by the FFC will be enabled under:

- the *Australian Crime Commission Act 2002* (Cth), section 7A(a) – Functions of the ACC; and,
- ACIC Project MINORU using the Special Australian Criminal Intelligence Commission Operation Determination (Serious Financial Crime) 2022 (SFC2022).

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

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

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

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

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

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

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

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

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

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.

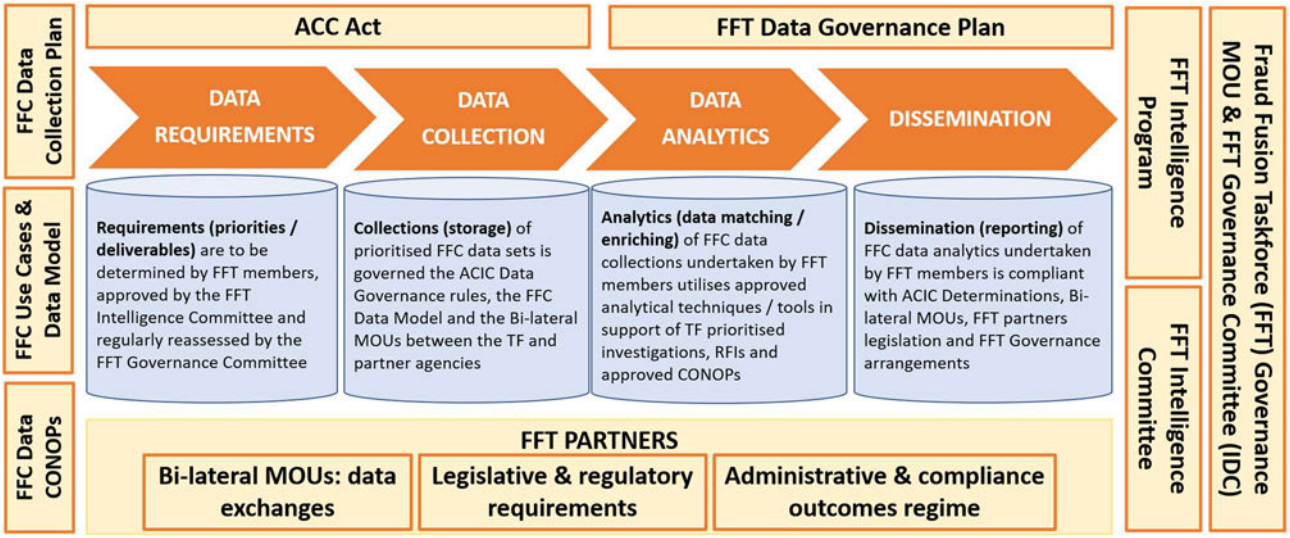
s 37(2)(b), s 47E(d)

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)

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

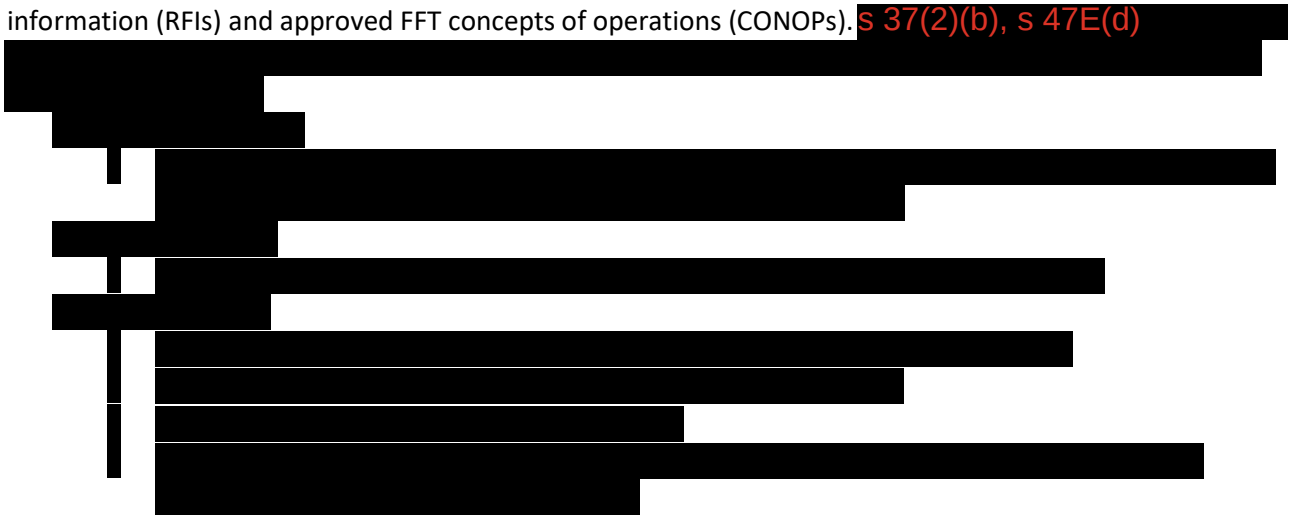
This section will provide details on the role all of the artefacts in delivering data governance across the intelligence cycle.

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.

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)



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)



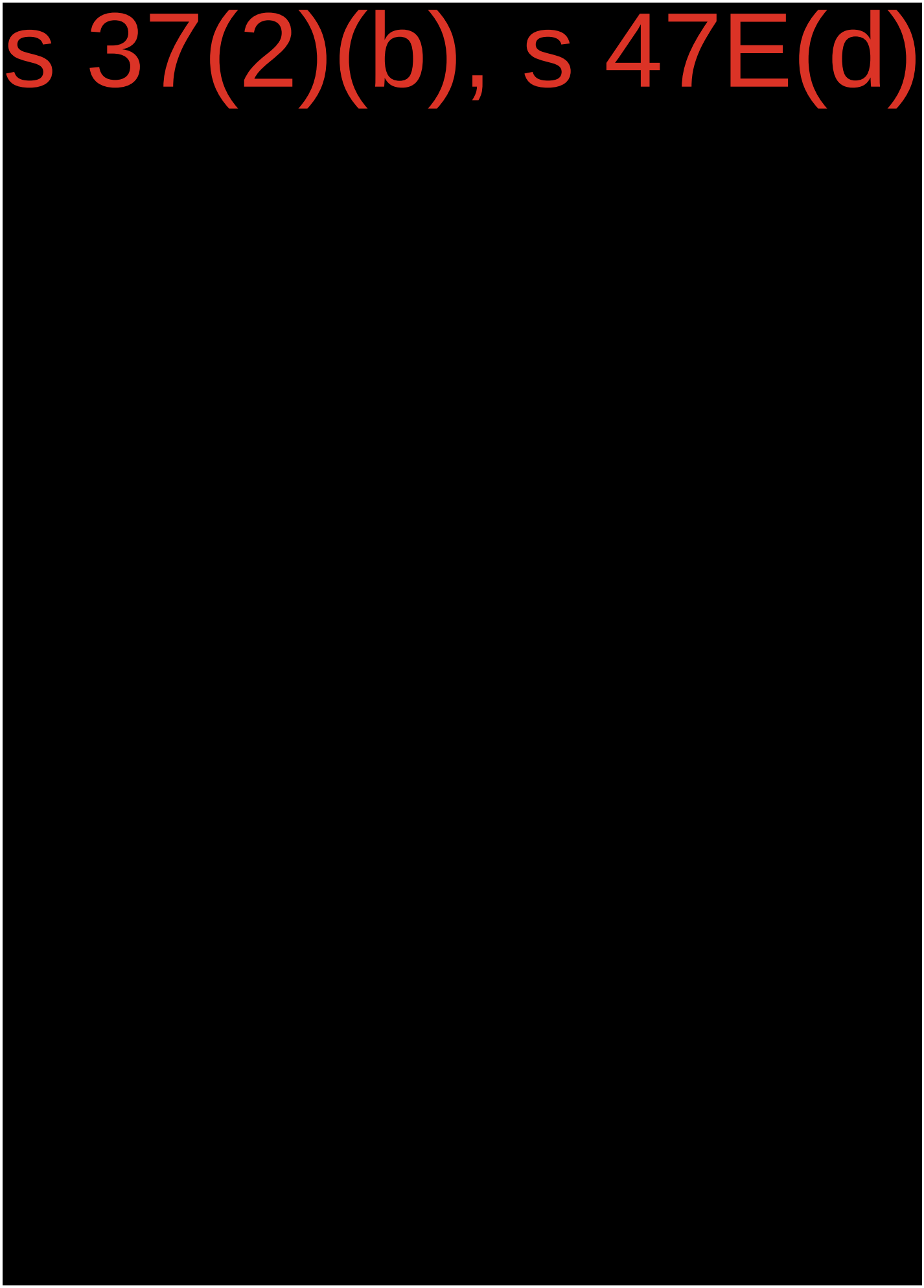
DATA COLLECTION (storage)

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)


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

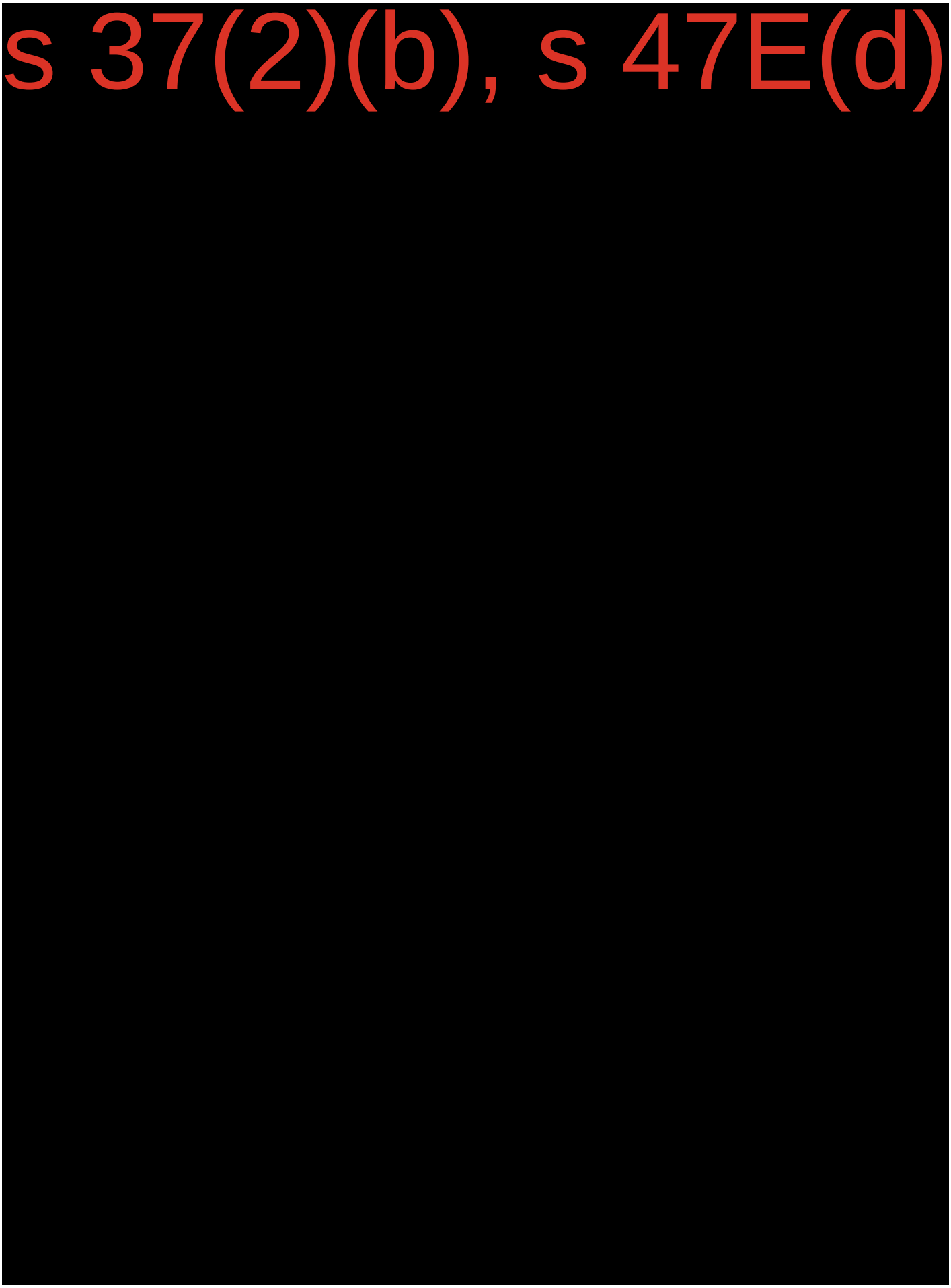
Access to disseminated FFC data sets

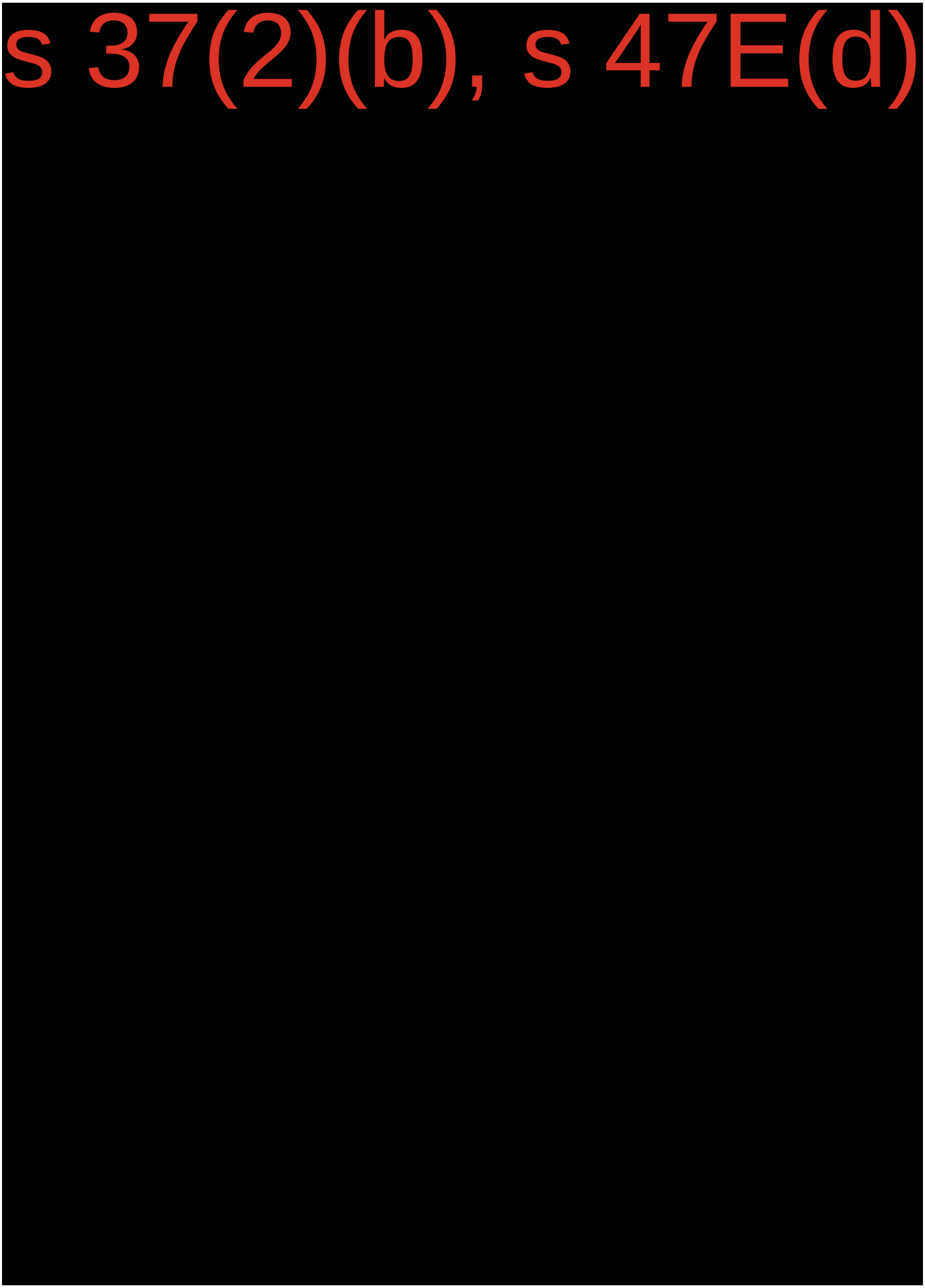
The central principle of disseminating FFC data sets to GP&P is to provide:

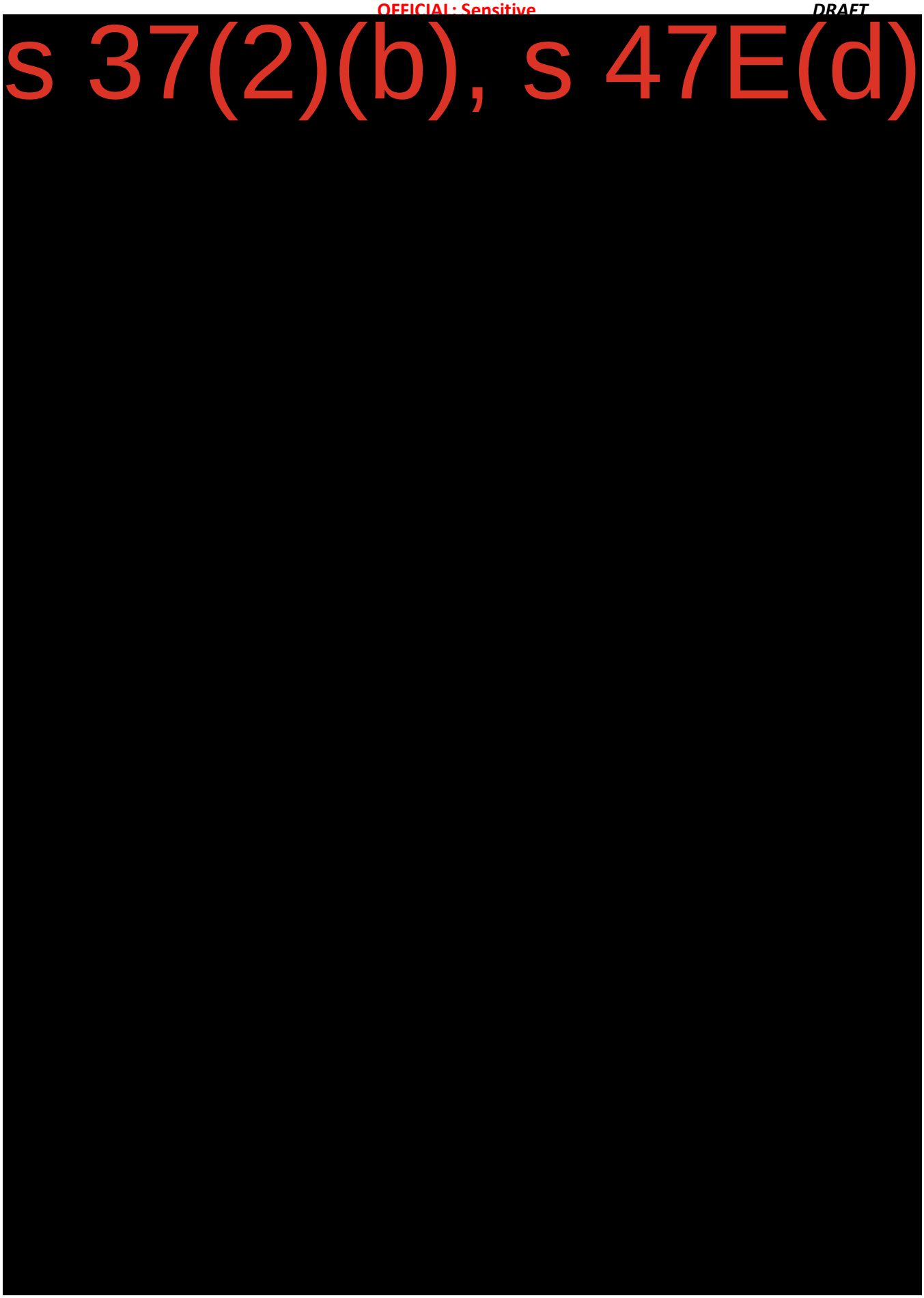
- guidance on the prioritisation of internal administrative and compliance activities; and,
- where GP&Ps can find additional information from other agencies on individual or corporate entities who are either looking to move into their GP&P or are already operating within GP&Ps

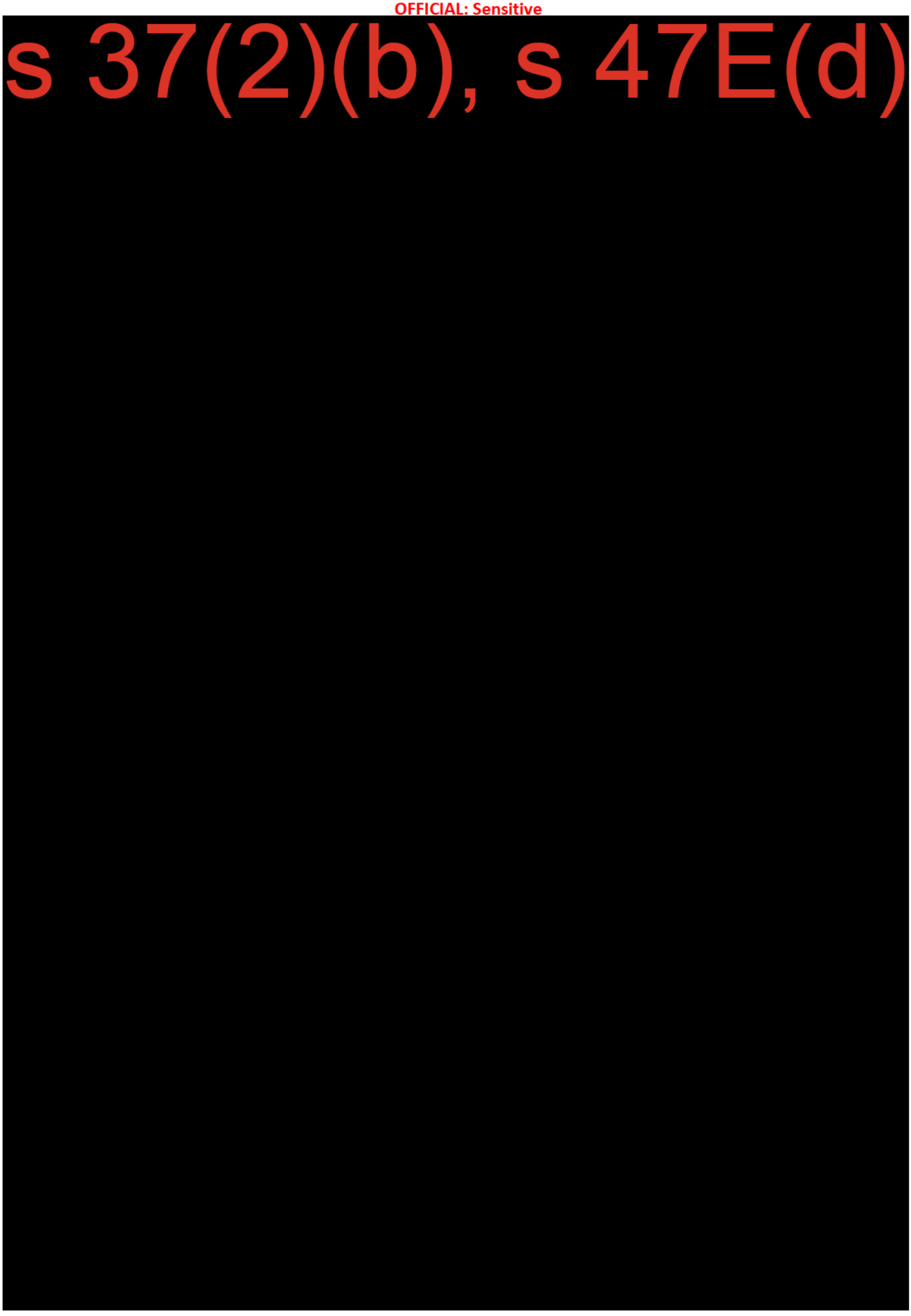
Broadly speaking, the specifics of any risk indicator data held against and individual or corporate entity within a GP&P will not be disseminated to any other agency. The exception to this principle will only be triggered if the legislative and regulatory framework governing a GP&P and the rules covering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

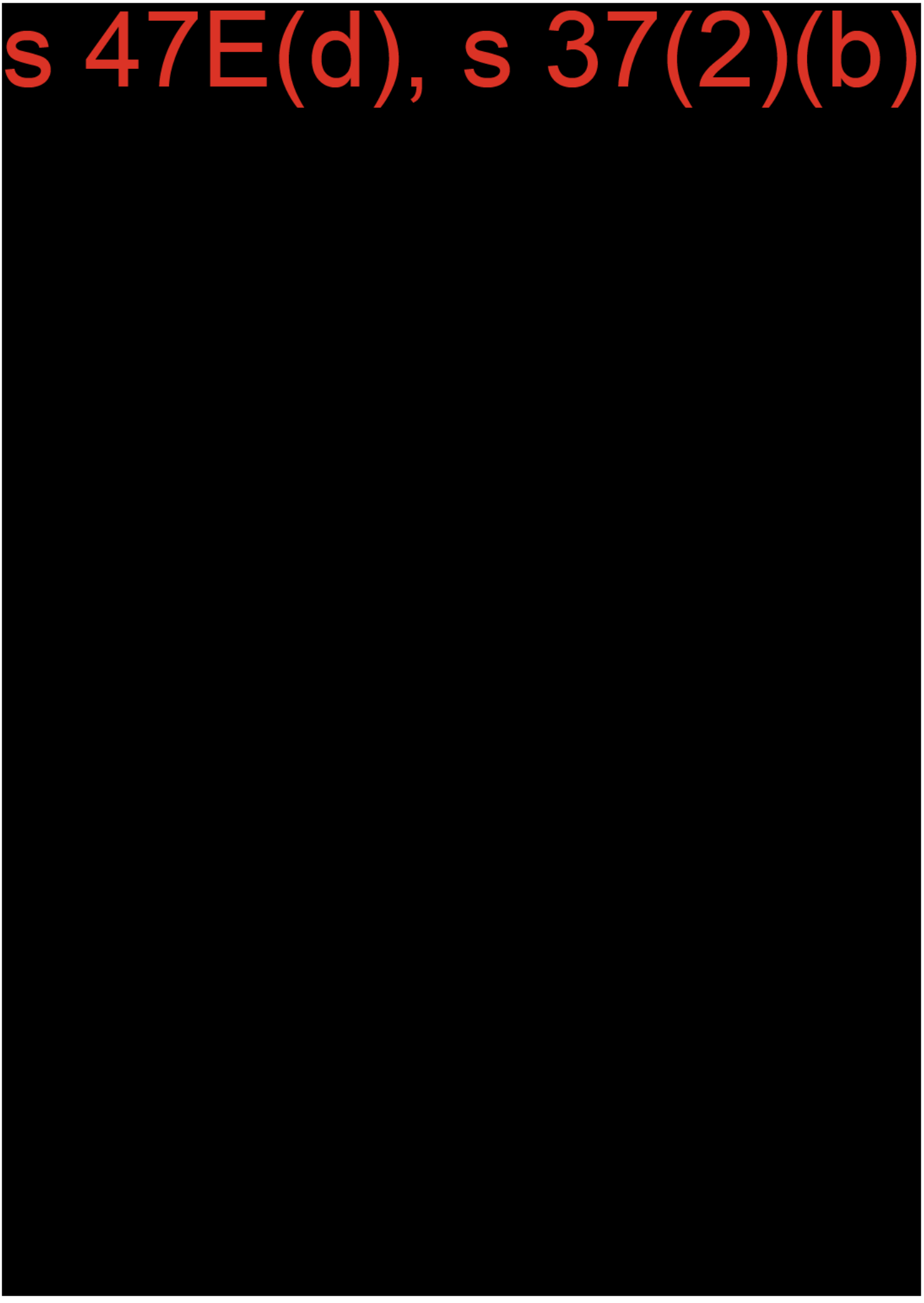
s 37(2)(b), s 47E(d)

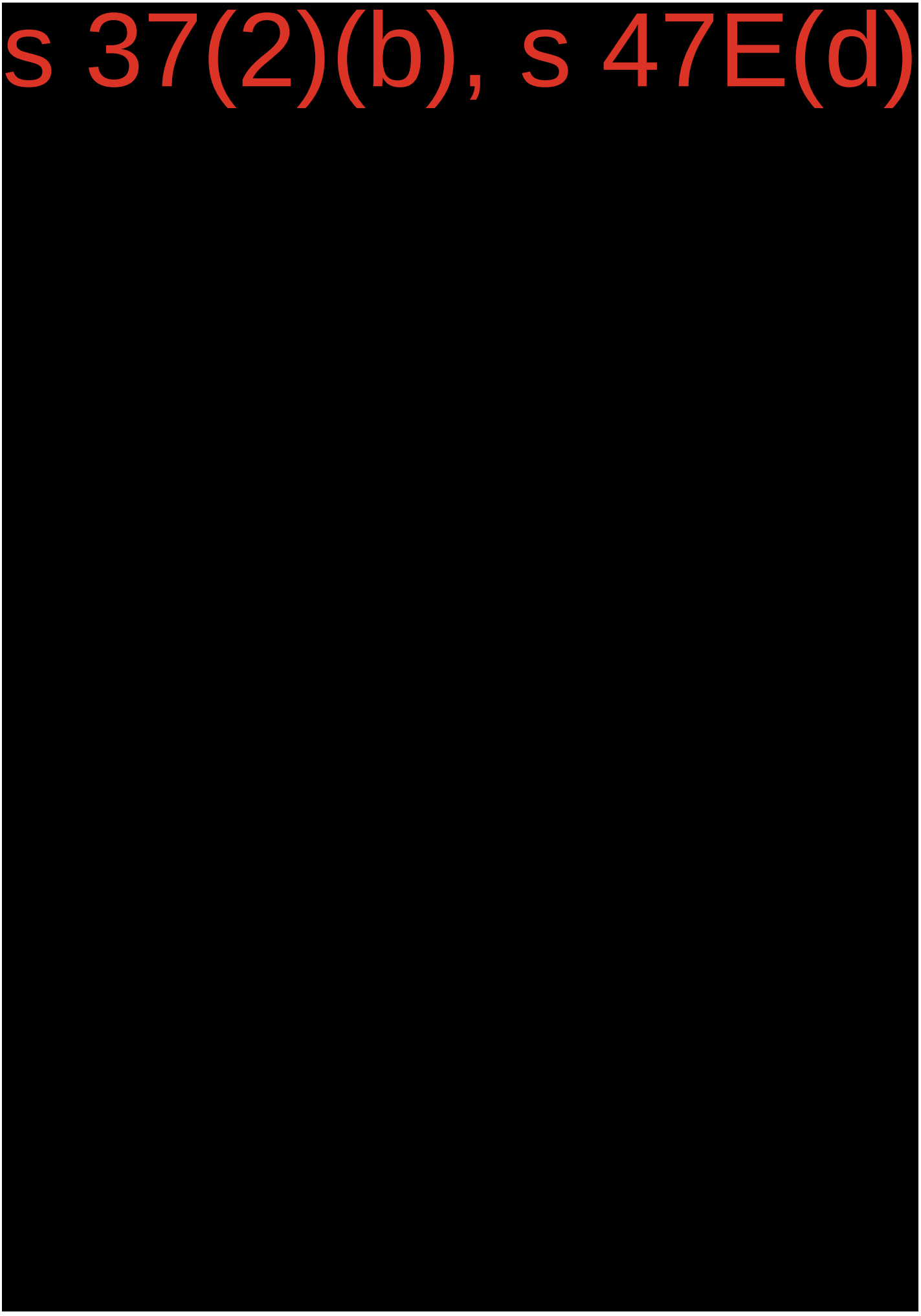

s 37(2)(b), s 47E(d)


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


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


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


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


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

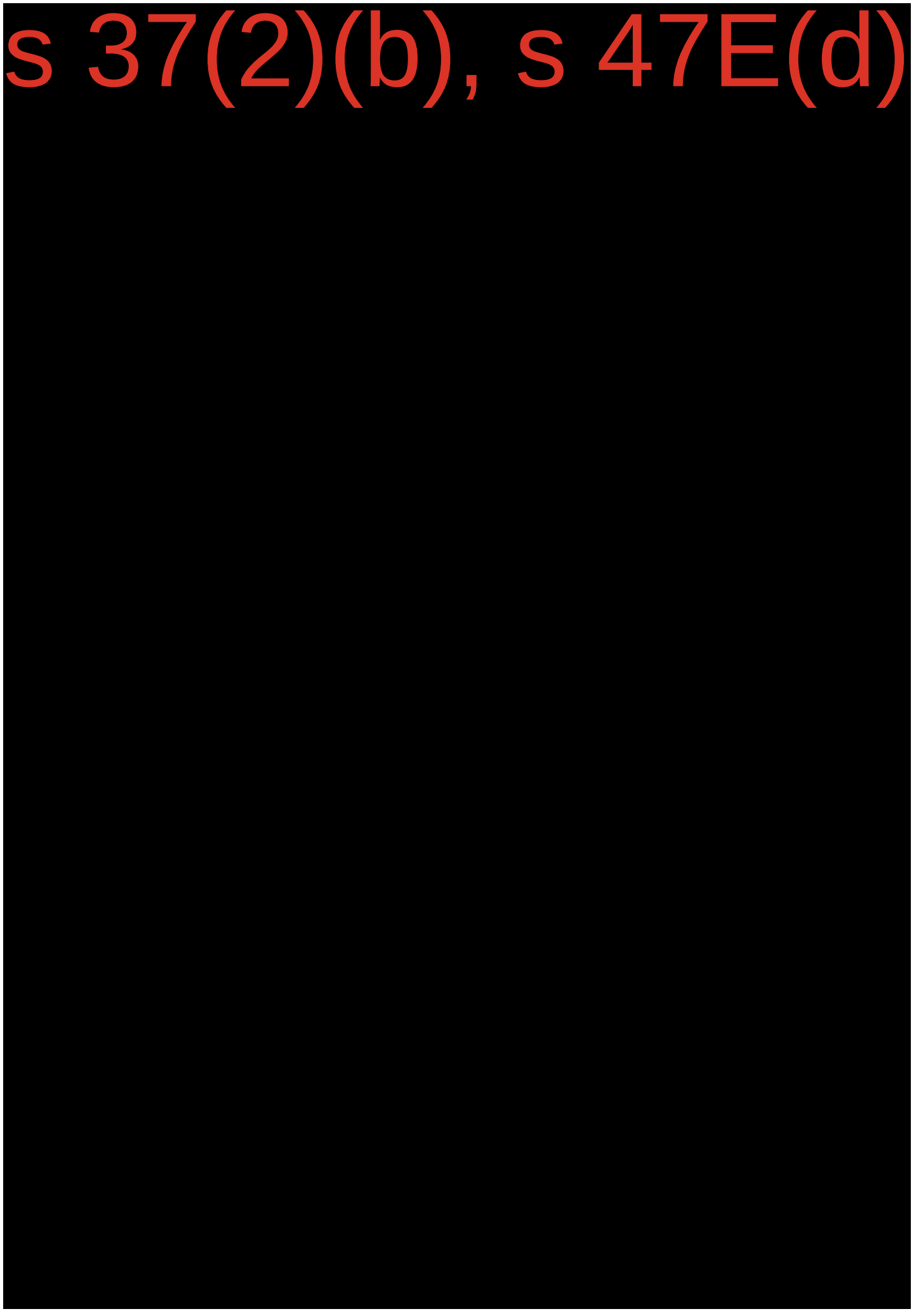
s 37(2)(b), s 47E(d)

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

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

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

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


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