

OFFICIAL: SENSITIVE

Fraud Fusion Taskforce Intelligence and Operations Committee Meeting of 21 May 2024

Agenda Item: 6 Data Sharing Update**Paper Type:** For Discussion**IOC Sponsor:** NDIA**Timing:** 21 May 2024**1. Purpose**

- 1.1. Provide an update on Data Sharing to the IOC.

2. Recommendation

- 2.1. IOC note updates for the:

- s22
- FFT Data Governance Framework.
- s22

s22

4. FFT Data Governance Framework

- 4.1. The NDIA has drafted the FFT Data Governance Framework (The Framework):

- The Framework is an overview of how FFT partners share datasets for the purposes of the FFT.
- Representatives from the Data Sharing Working Group have provided input into this Framework.
- The Framework does not cover each individual FFT partner's policies and procedures around sharing data and data governance.
- It is intended that IOC and SPC members provide feedback on this Framework, ahead of endorsement at the June IDC.

s22

OFFICIAL: SENSITIVE

OFFICIAL: SENSITIVE

Fraud Fusion Taskforce Intelligence and Operations Committee Meeting of 21 May 2024

s22

s22

7. Attachments

6A Appendix B – ACIC Fraud Fusion Centre Data Governance Plan

s22

Prepared by:	Author: s47F(1)	Approved by:
Division:	FFT & Integrity Capability Division, NDIA	Kitsa Papadopoulos
Phone:	s47F(1)	s47F(1)
Date prepared:	01/05/2024	
Version:	V2	

OFFICIAL: SENSITIVE

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:

NDIA	Services Australia
ACIC	Dept of Health and Aged Care
AFP	Attorney General's Dept
ATO	Dept of Veterans Affairs
AUSTRAC	Dept of Employment & Workplace Relations
ASIC	NDIS Quality & Safeguards Comm
	Dept of Education

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. s37(2)(b), s47E(d)

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 s37(2)(b), s47E(d) 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. s37(2)(b), s47E(d)

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. s37(2)(b), s47E(d)

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*.

OFFICIAL: SENSITIVE

Fraud Fusion Taskforce

Inter-Departmental Committee Meeting Minutes

13 June 2024, 1300-1500 AEST

Co-Chairs:

John Dardo, Deputy CEO Integrity Transformation and Fraud Fusion Taskforce, **NDIA**

Chris Birrer, Deputy CEO Payments and Integrity, **Services Australia**

Contact: s47F(1)

Secretariat, Fraud Fusion Taskforce, NDIA

P: s47F(1)

Members:

Australian Federal Police (AFP)

Adam Rice, Manager, Economic, Corporate Crime and Corruption, Crime Command (*proxy for Paula Hudson*)

Australian Criminal Intelligence Commission (ACIC)

Jennifer Hurst, Executive Director Intelligence Operations

Australian Taxation Office (ATO)

Louise Clarke, Deputy Commissioner Integrated Compliance (*proxy for John Ford*)

NDIS Quality and Safeguards Commission (NDIS Commission)

Catherine Myers, Deputy Commissioner Regulatory Operations (Registrar)

Attendees:

Australian Criminal Intelligence Commission (ACIC)

Anita Van Hilst, National Manager, Operational Strategy

s47F(1) Acting Director, Fraud Fusion Centre

Australian Federal Police (AFP)

s47F(1) Detective Acting Inspector

s47F(1) , Acting Superintendent

Attorney General's Department (AGD)

Pierre Skorich, Acting Assistant Secretary, Fraud Prevention and Anti-Corruption Branch

Australian Taxation Office (ATO)

Helen Wilson, Assistant Commissioner, System Integrity Program

s47F(1) , Director, Fraud Fusion Taskforce & Government Payments Program

s47F(1) , Acting Assistant Commissioner, Policy, Analysis & Legislation (*agenda 5 13:37 – 1400 AEST*)

OFFICIAL: SENSITIVE

OFFICIAL: SENSITIVE**Department of Social Services (DSS)**

Amanda Lee, Group Manager

s47F(1), Branch Manager, Audit and Assurance

National Disability Insurance Agency (NDIA)

Kitsa Papadopoulos, General Manager, Fraud Fusion Taskforce

Richard Honey, Branch Manager, Fraud Fusion Taskforce Capability Branch

s47F(1) Assistant Director, Governance, Assurance and Risk

s47F(1), Governance Officer, Governance, Assurance and Risk

s47F(1) Governance Officer, Governance, Assurance and Risk

Services Australia

Luke Morrish, Acting General Manager, Fraud Control and Investigations Division

Barb Smith, Acting National Manager, Intelligence Branch

s22 Director, Interagency Fusion, Intelligence Branch

Leo Lahey, National Manager of the Fraud Investigation Branch

TreasuryChris Leggett, Assistant Secretary, Law Division (*agenda 5 13:42 – 14:00*)**Apologies:****Australian Taxation Office (ATO)**

John Ford, Deputy Commissioner Integrated Compliance

Australian Federal Police (AFP)

Paula Hudson, Acting Assistant Commissioner

Ian McCartney, Deputy Commissioner

Kirsty Schofield, Assistant Commissioner

s47F(1), Inspector

Attorney General's Department (AGD)

Elizabeth Brayshaw, First Assistant Secretary, Integrity Frameworks Executive

s47F(1) Director, Capability and Communication

Department of Social Services (DSS)

Robyn Shannon, Deputy Secretary, Disability and Carers Stream

NDIS Commission

Mahashini Krishna, Assistant Commissioner, Regulatory Campaigns and Projects

TreasuryRichard Maher, Assistant Secretary, Tax System Branch, Personal and Indirect Tax and Charities Division, Revenue Group (*agenda 5*)**1. Welcome and apologies**

Co-chair Chris Birrer opened the meeting at 1:00pm AEST and welcomed members.
 13 June 2024 | FFT Inter-Departmental Committee Meeting

OFFICIAL: SENSITIVE

OFFICIAL: SENSITIVE

Taskforce Management Office (TMO) confirmed ahead of the meeting members and attendees held appropriate Security Clearances.

No conflict of interests was declared by members.

s22

OFFICIAL: SENSITIVE

OFFICIAL: SENSITIVE

s22

7. FFT Draft Data Governance Framework (endorsement)

Richard Honey presented the draft FFT Data Governance Framework for endorsement and provided IDC with a verbal update as follows:

- The Framework was widely consulted on via IOC and the DSWG, with opportunity to contribute open to all 19 FFT Members.
- The Framework is intended to foster a culture of trust and will apply to all agencies party to the FFT MOU, while acknowledging each agency is responsible for acting in accordance with their internal policies and procedures, and compliance with legal and ethical requirements.

IDC endorsed the FFT Data Governance Framework.

s22

OFFICIAL: SENSITIVE

OFFICIAL: SENSITIVE

s22

s22

s22

OFFICIAL: SENSITIVE

OFFICIAL: SENSITIVE

s22

OFFICIAL: SENSITIVE

OFFICIAL



Australian Government
Fraud Fusion Taskforce

Fraud Fusion Taskforce Data Governance Framework

Version: V1.0

Date: June 2024

Division: Fraud Fusion Taskforce Division

Commencement: Endorsed by IDC on 13 June 2024.

OFFICIAL

Contents

Fraud Fusion Taskforce Data Governance Framework	1
Contents	2
1. Introduction	3
1.1 Purpose	3
1.2 Context and environment	3
1.3 Scope	4
1.4 Consultation	5
1.5 Contact Officer	5
2. FFT Data Governance Approach	6
2.1 Australian Government Data	6
2.2 Data sharing in the FFT Context	6
3. Data Governance Landscape	8
3.1 Data Governance	8
3.2 Legislation	10
4. FFT Governance	11
4.1 FFT Ethics and Human Oversight Framework	11
4.2 FFT Risk Management Framework	11
4.3 Managing the Data Governance Framework	12
5. Appendices	14
Appendix A – FFT Background	14
Appendix B – Figure 1	16
Appendix C – Fraud Fusion Centre Data Governance Plan	16

OFFICIAL

1. Introduction

The Fraud Fusion Taskforce (FFT) is committed to establishing and maintaining appropriate governance arrangements to support data sharing activities between FFT partner agencies to achieve FFT objectives.

1.1 Purpose

The FFT Data Governance Framework (the/this Framework) outlines governance arrangements and aims to foster a culture of trust within the FFT partner agencies to promote safe and secure data and intelligence sharing.

The Framework:

- Supports the effective delivery of FFT activities.
- Contributes to FFT objectives as outlined in the FFT Memorandum of Understanding (MOU) clause 5(4) and the Data Sharing Working Group Terms of Reference.
- Outlines the different mechanisms that facilitate data and intelligence sharing between FFT agencies and into the Fraud Fusion Centre (FFC).
- Sets the agenda for an aligning legal mechanism to share information.

1.2 Context and environment

The FFT started in November 2022 and is a partnership between government agencies. **Appendix A** shows a list of current FFT partner agencies.

The purpose of the FFT is to improve payment integrity in government payment programs by detecting, preventing or reducing fraud and criminal activity within and

OFFICIAL

against government programs. As per the MOU clause 5(2), the FFT has several focus areas: strategy and intelligence and operational.

This Framework is part of a suite of FFT Assurance documentation to ensure the consistent and safe delivery of FFT activities. The suite of FFT Assurance documentation includes the:

- FFT Risk Management Framework and Strategic Risk Register (in development).
- FFT Ethics and Human Oversight Framework (in development).
- FFT Communications and Engagement Plan (endorsed November 2023).
- FFT Data Governance Framework (this document).

The FFT is operational during a time of significant change and reform across the whole of Government, including the recent [NDIS Review](#), [Review of Secrecy Provisions](#) and [Privacy Reform](#). As the FFT evolves, these elements may impact the context and environment the FFT operates.

1.3 Scope

This Framework applies to all FFT agencies who are parties to the FFT MOU. It does not replace or supersede any internal data governance arrangements held by individual FFT agencies.

This Framework relates to data sharing for FFT strategic priorities and dataset exchange. The Data Sharing Working Group (DSWG) and the FFT MOU (clause 14 – Data, Information sharing and security) are important reference points for FFT partners to refer to when considering data sharing.

Each partner agency is responsible for acting in accordance with their own:

- Data policies and frameworks.

OFFICIAL

- Data management (data quality, storage, stewardship and destruction).
- Data breaches.
- Individual legislative requirements relating to data sharing and data governance.
- Lawful and ethical data disclosures.

This Framework does not:

- Discount the accountability of individual agencies, their agency heads, and delegates to comply with individual legislative requirements, policies and procedures relating to data sharing and data governance.
- Cover case-level operational data sharing where the sharing has occurred under a pre-existing data sharing arrangement.

1.4 Consultation

The Framework has been developed in consultation with the Parties to the MOU, FFT Inter-Departmental Committee (IDC), Intelligence and Operations Committee (IOC), Strategic Prevention Committee (SPC), FFT Data Sharing Working Group (DSWG) and the Taskforce Management Office (TMO).

1.5 Contact Officer

s47E(d)

OFFICIAL

2. FFT Data Governance Approach

2.1 Australian Government Data

Australian Government data encompasses all data lawfully collected, created or held by a Commonwealth body, or on its behalf. Data can include a wide range of topics, from data dealing with the weather, personal and business data, through to freight and traffic movements, and agricultural yields.¹

The Australian Government is developing a whole-of-government Data Governance Framework to define common rules, processes, and accountabilities for adoption across the Australian Public Service to ensure privacy and compliance of government data is maintained.²

In the FFT, there are a variety of data types and different ways to represent data. This framework covers data governance relating to FFT strategic priorities and dataset exchange.

This Framework does not supersede each partner agency's own data governance plans and/or frameworks.

2.2 Data sharing in the FFT Context

In accordance with the FFT MOU, datasets are collected and shared to support the FFT to identify, understand, target, prevent, and/or disrupt existing or emerging fraudulent activities and serious and organised crime entities, operating within identified government payment programs.

¹ *Share Data*, [Share Data | Office of the National Data Commissioner](#), Accessed 5 April 2024.

² *Australian Government Data and Digital Strategy*, [Data Governance Framework \(New\) | Data and Digital](#), Accessed 4 April 2024.

OFFICIAL

OFFICIAL

s47E(d)

This Framework acknowledges each partner agency has their own policies and procedures for data sharing and disclosures. Specific partners will have their own Request for Information (RFI) process for requesting datasets. Partner agencies should refer to existing FFT resources (i.e. DSWG and FFT MOU) when considering data sharing. Partner agencies should also seek internal or external legal advice to ensure the proposed data sharing arrangement is aligned to individual legislative requirements, policies and procedures relating to data sharing and data governance.

s47E(d)

OFFICIAL

Further work is underway to understand the delays in dataset exchange with the FFC. Further suggestions will be made as part of work underway in the Attorney-General's Department.

3. Data Governance Landscape

3.1 Data Governance

Intelligence and Operations Committee Data Sharing Working Group

The Intelligence and Operations Committee (IOC) Terms of Reference (ToR) sets out that working groups can be established to facilitate the operational objectives of the IOC as a sub-committee of the Inter-Departmental Committee (IDC).

Under Subclause 3(7) of the IOC ToR, the IOC may appoint a working group/s to assist with carrying out its function.

The Data Sharing Working Group (DSWG) provides oversight to specific areas of strategic operations and is responsible for identifying and managing data sharing governance arrangements that impact FFT activities, operations, and decisions. These are reported through meeting minutes and managed through regular update and review of the FFT Data Sharing Register.

The DSWG provides data sharing and governance oversight to IOC and the Strategic Prevention Committee (SPC).

Figure 1 at **Appendix B** is an image that shows how the different strategic and operational elements of the FFT interact with the different FFT committees and working groups.

s47E(d)

OFFICIAL

s47E(d)

Fraud Fusion Centre Data Governance Plan

The FFC has been established as the hub for cross-government intelligence and tactical collaboration. The FFC is led by the Australian Criminal Intelligence Commission (ACIC) and assists with data and intelligence collection and analysis aimed at enhancing understanding of key vulnerabilities and identifying new disruption opportunities.

The FFC Data Governance Plan (**Appendix C**) establishes key principles and governance to the collection, use, storage, disclosure and destruction of the data exchanged within the FFC. The key objectives of the FFC Data Governance Plan include:

- 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.

OFFICIAL

OFFICIAL

- 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.

3.2 Legislation

The sharing and handling of data across all FFT agencies must comply with individual legislative requirements, policies and procedures relating to data sharing and data governance.

FFT decision-making regarding data must be made in accordance with Legislation associated with Data Governance, including but not limited to:

- *Data Availability and Transparency Act 2022 (Commonwealth)*
- *Privacy Act 1988 (Commonwealth)*
- *Public Governance, Performance and Accountability Act 2013 (Commonwealth)*
- *Archives Act 1983 (Cth)*
- *Australian Government Protective Security Policy Framework*
- *Performance and Accountability Act 2013.*

OFFICIAL

4. FFT Governance

4.1 FFT Ethics and Human Oversight Framework

The FFT is committed to applying a sound ethical framework to support ethical conduct and decision making in relation to its activity and to achieve its purpose and objectives.

The FFT Ethics and Human Oversight Framework outlines the FFT's ethical decision-making framework and how ethical values and principles guide cross-agency decision-making to support ethical conduct and decision-making.

Some considerations that need to be addressed in FFT activity to achieve ethically sound governance and operations include:

- Ensuring safety and wellbeing of participants and recipients of Australian government payment programs.
- Recognising how FFT activity (decisions, actions and operations) may impact the community and individuals.
- Ensuring a human oversees or reviews decisions if agencies use automation to gather and analyse information.
- Ensuring data and information is kept safe, protected and disclosed securely.

Partner agencies will also be informed by their own individual data ethic frameworks to inform decision-making by the FFT.

4.2 FFT Risk Management Framework

The FFT is committed to establishing an effective system of oversight to identify, assess, manage, and report on material shared risks in relation to the FFT's activities in achieving its goals and objectives.

OFFICIAL

The FFT Risk Management Framework outlines the FFT's approach to embedding effective risk management in relation to FFT activities, to ensure appropriate oversight of shared risks is maintained in achieving its goals and objectives. The FFT Risk Management Strategy and FFT Strategic Risk Register supports the FFT Risk Management Framework.

The FFT Strategic Risk Register includes material shared strategic risks³ to ensure the IDC, and other FFT governance committees, maintain appropriate oversight to support ethical, risk balanced decision-making in relation to the risks affecting multiple agencies in the taskforce in the execution of its purpose, including data sharing activities between FFT agencies.

4.3 Managing the Data Governance Framework

Reporting

Timely and accurate reporting is essential for IDC and FFT Governance Committees to maintain oversight and ensure the FFT is complying with its Frameworks and appropriately managing data governance, any associated risks and ethical issues, and is supported to make informed decisions on data sharing.

The TMO will coordinate FFT assurance activity to monitor compliance with FFT Frameworks and Registers. This includes compliance with the Data Governance Framework. This will ensure the IDC has effective oversight and can monitor the successful implementation of the Framework.

The FFT assurance process will involve the TMO seeking quarterly updates on data sharing from the FFT governance committees, working groups and partner agencies.

³ Significant risks that extend across entities and may prevent the FFT from executing or achieving its strategic objectives due to internal and external factors.

OFFICIAL

This information will inform the assurance reporting dashboard for IDC. TMO will prepare the paper and assurance reporting dashboard for quarterly reporting to IDC.

Review

The FFT is committed to continuous improvement. The TMO will coordinate a review of this Framework at least annually to ensure controls continue to be relevant, effective and address emerging data sharing risks including substantial changes in the FFT's structure, functions, or activities.

This will ensure that:

- The FFT Data Governance Framework and respective registers reflect the FFT's operating environment.
- Data Governance processes continue to be effective.
- Data sharing reporting continues to provide information necessary to enable delegates to make informed decision making, maintain appropriate oversight, and enable continuous improvement; and
- Data Governance continues to effectively contribute to delivering the FFT's purpose and objectives.

The IDC will be provided with a review report and the IDC will need to endorse any changes made to the FFT Data Governance Framework.

OFFICIAL

5. Appendices

Appendix A – FFT Background

The Fraud Fusion Taskforce (FFT) is a multi-agency collaboration to strengthen the Government's approach to sharing data intelligence and coordinating action of fraud committed by serious and organised crime entities with the aim of reducing fraud across government payment programs.

The FFT is co-led by National Disability Insurance Agency (NDIA) and Services Australia and currently includes the following agencies:

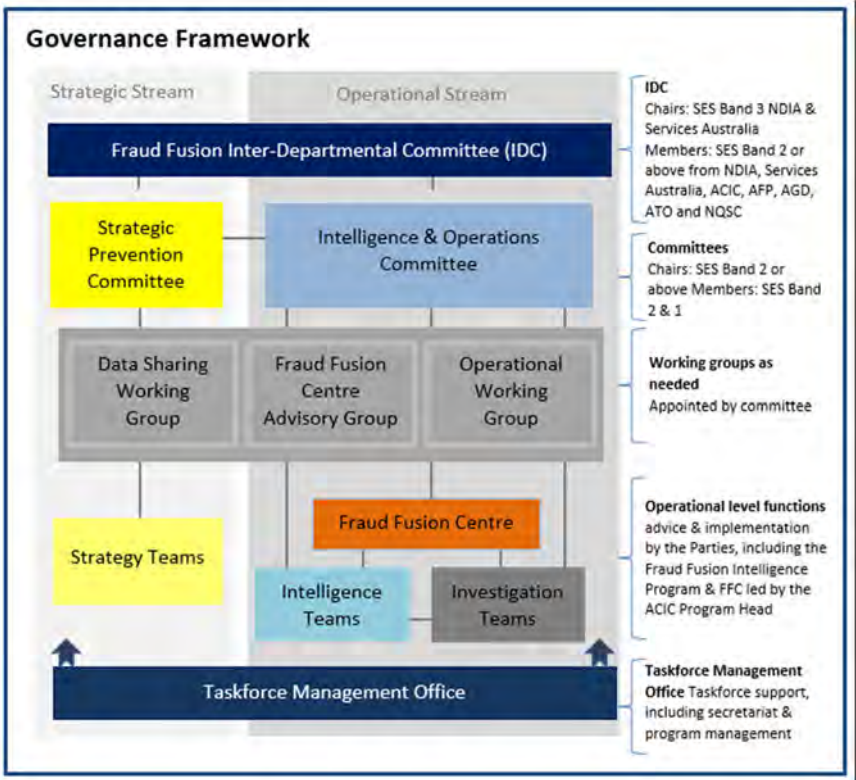
Stakeholder category	Agency
FFT lead agencies	• National Disability Insurance Agency (NDIA) • Services Australia
FFT Inter-Departmental Committee agencies	• NDIA • Services Australia • Australian Taxation Office (ATO) • Australian Criminal Intelligence Commission (ACIC) (responsible for Fraud Fusion Centre (FFC)) • Australian Federal Police (AFP) • NDIS Quality and Safeguards Commission (NQSC) • Attorney-General's Department (AGD) – Commonwealth Fraud Prevention Centre (CFPC)

OFFICIAL

Stakeholder category	Agency
Other FFT partner agencies	• Australian Securities and Investments Commission (ASIC) • Australian Transaction Reports and Analysis Centre (AUSTRAC) • Commonwealth Director of Public Prosecutions (CDPP) • Department of Employment and Workplace Relations (DEWR) • Department of Veterans' Affairs (DVA) • Department of Education (DoE) • Department of Health and Aged Care (DoHAC) • Department of Social Services (DSS) • Australian Charities and Not for Profit Commission (ACNC) • Australian Skills Quality Authority (ASQA) • National Indigenous Australians Agency (NIAA) • Professional Services Review (PSR).

OFFICIAL

Appendix B – Figure 1



Appendix C – Fraud Fusion Centre Data Governance Plan

Refer to PDF document attached.

OFFICIAL