Document 1

Privacy Impact Assessment

Data sharing agreement between the Department of Education and the Australian Bureau of Statistics (executed in January 2024)

In accordance with the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (the Code), the Department of Education (the department) is undertaking a Privacy Impact Assessment (PIA) to determine whether this initiative is compliant with the *Privacy Act 1988* (Privacy Act), including the Australian Privacy Principles (APPs). This PIA will identify privacy risks associated with the initiative and counteractive steps that the department should take to avoid, minimise or mitigate identified privacy risks.

Project or initiative

Initiative description
A data sharing agreement between the Department of Education (the department) and the Australian Bureau of Statistics (ABS) was executed in January 2024 (the Agreement). Under section 168(1)(b)(i) of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Administration Act), the Secretary of the department will disclose unit record child care data, which constitutes protected information, to the Australian Statistician as the head of the ABS for the purposes of the ABS. The purposes of the ABS include official statistics and statistical research purposes of the *Census and Statistics Act 1905* as specified at Annex 1 of the Agreement. In accordance with section 162(2)(e) of the Administration Act, a person may (a) make a record of the protected information, (b) disclose the information to any person, or (c) otherwise use the information, for the purposes for which it was disclosed under s 168 (ie, for the purposes of the ABS). The Agreement limits this to the ABS purposes specified at Annex 1. The Agreement will enable approved departmental officers, approved employees of Commonwealth, state and territory agencies and approved non-government researchers to access de-identified unit record data in the DataLab environment for approved research purposes. The Agreement will improve the quality of macroeconomic statistics, the quality and timeliness of statistics related to families and child care, and the evidence base for understanding what early childhood education and care (ECEC) experiences make a difference to children's outcomes. It also

reduces the cost of sharing and using data without compromising on privacy protections, by sharing data under a single agreement for an agreed set of approved statistical purposes.

The department has been providing these datasets to the ABS for years for use in the National Early Childhood Education and Care Collection, the Consumer Price Index (CPI) and various data linkage projects. The department was previously providing these datasets to the ABS under public interest certificates.

The department has similarly been authorising non-ABS researchers to access child care data for approved research purposes via the ABS DataLab under public interest certificates.

This PIA examines the department's compliance with the APPs in relation to the provision of information to the ABS in accordance with the Agreement. This PIA does not examine the ABS' compliance with the APPs.

Key dates and timeframes

- The Agreement was executed on 18 January 2024 and will end on 18 January 2028.
- The Agreement will be reviewed annually in October.
- The data will be supplied to the ABS via a staged approach. The first tranche of data is expected to be disclosed to the ABS between March and June 2024.
- Data will be disclosed to the ABS annually, with more frequent extracts subject to agreement between the department and the ABS.
- The ABS will submit a report to the department biannually which outlines information on the projects that have been undertaken using the data, a summary of findings from those projects (if available) and a summary of any data breaches that have occurred during the reporting period.

Stakeholders

The department has consulted the following stakeholders.

Stakeholder name	Response to consultation
Australian Bureau of Statistics	Representatives from the department's Data and Delivery Support Branch engaged with ABS staff from mid-2021 to negotiate the terms of the Agreement. Dr David Gruen, Australian Statistician, executed the Agreement on 18 January 2024. Those same departmental representatives are meeting with ABS staff regularly from February 2024 to confirm the data specification under the Agreement and the logistical arrangements for transmission.
Australian Government Solicitor	The department's Child Care Legal team sought advice from the Australian Government Solicitor in 2023 to inform the final terms of the Agreement.

State and territory governments	The department is consulting with state and territory governments on the data specification to be supplied to the ABS via the Data Sharing Working Group established under the Early Childhood Policy Group.

Personal information flows

The department will handle personal information[1] in the initiative as follows.

Type of information	Collect	Use	Disclose	Store	Destroy	De-identify
Names	☐	☑	☑	☑	☑	☑
Addresses	☐	☑	☑	☑	☑	☑
Dates of birth	☐	☑	☑	☑	☑	☑
Sex or gender	☐	☑	☑	☑	☑	☑
CRNs	☐	☑	☑	☑	☑	☑
Financial information	☐	☑	☑	☑	☑	☑
Racial or ethnic origin	☐	☑	☑	☑	☑	☑

Collection	The department will not collect personal information as part of this initiative. Personal information is stored in Services Australia's Enterprise Data Warehouse (EDW), however, the department considers that it already 'holds' this information given that the department has the right to deal with the data stored in the EDW that it is responsible for administering under the family assistance law.
Use	The department will use the data to prepare it for disclosure to the ABS. The department will extract the data from Services Australia's EDW and clean and transform it into tables, including deriving fields, applying counting rules and geocoding data. Some data may be extracted directly from the Child Care Subsidy IT system where it cannot be located in the EDW. The ABS will provide support to the department to establish appropriate checks and cleaning methods. The department will also source National Workforce Census services files and workers files directly from the National Workforce Census results stored internally. The ABS will use the data for the purposes specified in Annex 1 of the Agreement.
Disclosure	The department will disclose data to the ABS via secure file transfer. Informatica is used for transmittal, which has been built and configured

[1] 'Personal information' is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

	in accordance with the Australian Cyber Security Centre's Information Security Manual (ISM).
Storage	The data is initially stored in Services Australia's EDW and the department's secure electronic environment (SAS grid) where access is restricted.
Destruction	Personal identifiers will be provided to the ABS separately for data linkage purposes only and destroyed immediately after a de-identified linkage concordance is established. An encrypted PLIDA concordance file may be retained for approved purposes as outlined in Annex 1 of the Agreement. The destruction is consistent with the *Archives Act 1983* (Archives Act).
De-identification	As above, personal identifiers will be provided to the ABS separately for data linkage purposes only and destroyed immediately after a de-identified linkage concordance is established. The de-identification is consistent with the *Archives Act 1983* (Archives Act). The department and ABS have agreed that Customer Reference Numbers (CRNs) will be the primary means for linking data, however, names, dates of birth, gender and addresses may also be supplied to improve linkage results.

Analysis of APP compliance

The below table analyses the compliance of the initiative against each APP.

APP	Analysis
APP 1 – open and transparent management of personal information The APP entity must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way.	The department has a Privacy Policy in place to ensure it manages personal information in an open and transparent way, consistent with APP 1. The department will also list this PIA in the register of PIAs on its website in accordance with s 15 of the Privacy Code. This initiative is also underpinned by a data sharing agreement which outlines the data which will be disclosed to the ABS and the expectations for data handling within this project. The existence of a data sharing agreement promotes openness and transparency about how personal information will be handled in this project.
APP 2 – anonymity and pseudonymity Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter, unless an exception applies.	Personal information is not being collected by the department as part of this initiative and the department is therefore not "dealing with" individuals in the context of disclosing information to the ABS.

APP 3 – collection of solicited personal information Any personal information collected (other than sensitive information) must be reasonably necessary for or directly related to one or more of the department's functions or activities. The department must not collect sensitive information[2] about an individual unless one of the exceptions listed in APP 3.3 or APP 3.4 applies, such as if the individual consents and the information is reasonably necessary for or directly related to one of more of the department's functions or activities. Personal information can only be collected by lawful and fair means. Personal information about an individual must only be collected from the individual unless one of the exceptions in APP 3.6 applies.	Personal information is not being collected by the department as part of this initiative. The ABS will need to ensure that it is collecting personal information in accordance with APP 3, but this is outside the scope of this PIA.
APP 4 – dealing with unsolicited personal information Where an APP entity receives unsolicited personal information,[3] it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the APP entity must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.	As personal information is not being collected by the department as part of this project, it is unlikely or unforeseeable that the department will receive unsolicited personal information. In relation to the provision of data to the ABS, a procedure is in place under the Agreement to deal with the receipt of unsolicited information by the ABS. The ABS will check for unsolicited data immediately upon receipt. In the case that the ABS finds unsolicited information the department will be advised and the ABS will securely delete the unsolicited information.
APP 5 – notification of the collection of personal information Where the department collects personal information about an individual, it must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of the matters listed in APP 5.2. The department must provide notification before, or at the time it collects personal information. If this is	The department is not collecting personal information for the purpose of this project, rather, the department is disclosing personal information it already holds to the ABS. The requirement in APP 5.2(f) relates to notifying individuals of the recipients or types of recipients to which the department 'usually

[2] Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

[3] Personal information that the department did not solicit or ask for from individuals.

not practicable, notification should be provided as soon as practicable after collection. The matters listed in APP 5.2 include: • the department's and, if relevant, its contracted service provider's identity and contact details • the facts and circumstances of collection • whether the collection is required or authorised by law • the purposes of collection • the consequences if personal information is not collected • the department's and, if relevant, it's contracted service provider's usual disclosures of personal information of the kind collected • information about the department's privacy policy • whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located. A privacy statement template is available on the intranet.	discloses' personal information of the kind it collects. The ABS will need to consider its own obligations under APP 5 as the entity collecting the personal information. To the extent that the department is also responsible for notifying individuals of matters listed in APP 5.2 in relation to the project, the department's Privacy Policy, which is available on the department's website, relevantly states that: • the department collects, holds, uses and discloses personal information for purposes including policy development, research and evaluation; and data sharing with other Australian Government agencies including data sharing or data integration with the Australian Bureau of Statistics for the Multi-Agency Data Integration Project (now known as the Person Level Integrated Data Asset) • the department collects personal information under legislation it administers, including in relation to the child care subsidy, additional child care subsidy, child care providers and child care services • the department may use and disclose personal information where it is required or authorised by law. To the extent the department is sharing data collected through Early Childhood Education and Care National Workforce Censuses undertaken in 2024, 2021 and 2016, the department has also notified participants in the Census that "information collected as part of the Census may also be disclosed to the ABS for the purposes of the ABS, including but not limited to statistical analysis of child care providers or services". There is no record of privacy notices being disseminated for the 2013 and 2010 National Workforce Census collections, however the department is only planning to share data from the 2024 and 2021 censuses.

APP 6 – use or disclosure of personal information The department can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. Exceptions permitting use or disclosure for a secondary purpose include, for example, where: • the individual consents to the use or disclosure • the individual would reasonably expect the use or disclosure, and the secondary purpose is related to the primary purpose or, in the case of sensitive information, directly related to the primary purpose • the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order. This flowchart determines if personal information can be used or disclosed (in Australia).	The department collected the personal information for the primary purpose of administering the Child Care Subsidy and collecting workforce information via the National Workforce Census to inform ECEC policy development. As noted above, the department has also previously notified participants of the 2024, 2021 and 2016 National Workforce Censuses that information collected as part of the Census may be disclosed to the ABS for the purposes of the ABS, including but not limited to statistical analysis of child care providers or services. As a result, it is likely that in these circumstances the department is disclosing this specific information for the same primary purpose for which it was collected. However, to the extent the department is proposing to disclose datasets that were not subject to this (or a similar) privacy notice, including the 2013 and 2010 National Workforce Censuses, the department will use and disclose personal information in this initiative for a different (ie secondary) purpose. The department will use the personal information to prepare it for disclosure to the ABS. The department will disclose the data for the purposes of the ABS. The Agreement lists the ABS purposes for which the data may be used at Annex 1, which include linking and analysing data for use in official statistics and approved research projects, and to enable approved employees of Commonwealth, state and territory agencies and non-government researchers to access the data from the ABS for approved purposes. The department's use and disclosure of personal information for the secondary purpose (ie, for the purposes of the ABS) is consistent with APP 6.1 because the use or disclosure of the personal information is required or authorised by an Australian law, namely section 168(1)(b)(i) of the Administration Act, which authorises the Secretary of the department to

	disclose protected information to the Australian Statistician of the ABS for the purposes of the ABS. In doing so, the Secretary must act in accordance with any guidelines (if any) in force under section 169 (section 168(3)). No guidelines are currently in force. Further, paragraph 162(2)the authorises a person to use and disclose protected information for the purpose for which the information was disclosed under section 168 (ie, for the purposes of the ABS). In terms of the ABS' further disclosure of the information, the Agreement provides that where a project involves the 'on-sharing of data' to employees of the Commonwealth, state and territory agencies and non-government researchers, the ABS must ensure that the on-disclosure of protected information is 'for a purpose of the ABS within its legislative framework' (p 5). Under the Agreement, the ABS can only on-share *de-identified* data.
APP 7 – Direct Marketing An organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies, such as where the individual has consented.	The department is not one of the agencies specified under section 7A of the Privacy Act. Therefore, APP 7 does not apply to the department.
APP 8 – cross-border disclosure of personal information Before the department discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent. If the department discloses personal information to an overseas recipient, it is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (see s 16C of the Privacy Act). **Publication of personal information on a public facing website could constitute a cross-border disclosure of personal information where that website can be accessed by people located overseas.**	All data being shared with the ABS is located within Australia and will not be disclosed overseas. Any information or reports published by the ABS about the data would only include de-identified information provided by the department as part of this project and would not be attributable to a specific individual. The Agreement enables the ABS to publish aggregate statistical analysis of the data for approved projects, as long as the analysis is no longer 'about a person'. This will ensure that published outputs do not contain protected or personal information. The ABS will also provide the department with an opportunity to provide feedback on any proposals to publish new statistical information that directly uses the CCA (Child Care administrative) data.

APP 9 – adoption, use or disclose of government related identifiers An organisation must not adopt, use or disclose a government related identifier of an individual as its own identifier of the individual unless an exception applies. APP 9 generally applies only to organisations and does not in most instances apply to the department. However, separate legislative restrictions apply to the use of government related identifiers.	The department is not one of the agencies specified under section 7A of the Privacy Act. Therefore, APP 9 does not apply to the department.
APP 10 – quality of personal information The department must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. The department must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.	The following steps will be taken to ensure that the personal information the department handles in this initiative is accurate, up-to-date, complete and relevant, having regard to the purpose for which it is being handled: • The data will be drawn from Services Australia's EDW and the National Workforce Census results held internally. • Prior to providing the data to the ABS, the department will clean and validate the data to ensure its quality and to prevent the supply of unsolicited data to the ABS. The ABS will support the department to establish appropriate checks and cleaning methods. • Data table descriptions and data dictionaries will be developed and supplied with the data to ensure that the data being disclosed can be interpreted appropriately and analysed accurately.
APP 11 – security of personal information An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that the information is de-identified, unless an exception applies.	The following steps will be taken to protect the personal information handled by the department in this initiative from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure: *Steps undertaken by the department* • Data to be disclosed to the ABS is held by the department in a secure electronic environment and is only accessible by a limited number of officers who require

	access, with two factor authentication required. • All relevant departmental officers have completed mandatory privacy training, hold a minimum of a Baseline security clearance and can only access information on a 'need to know' basis. • In the event of a data breach, the department is bound by its responsibilities under the Privacy Act. The relevant staff members are also aware of the department's Data Breach Response plan and their responsibilities under that plan. • The data sharing agreement limits the use of the datasets and prohibits the publication or further disclosure of the datasets by the ABS. • In the event that any variations or changes to the data disclosed under the Agreement are required, as outlined in Annex 2, departmental staff will seek authority from the Secretary of the department (see section 5, p 9) in accordance with the Agreement. *Steps undertaken by the ABS* • The ABS' transmission, storage and access environments meet or exceed the Australian Information Security Standard (AS/NZS 4444). • Informatica is used for transmittal, which has been built and configured in accordance with the Australian Cyber Security Centre's Information Security Manual (ISM). The security of the data connection, accounts and usernames are maintained in accordance with the ISM and industry best practice methods. Further checks of file integrity and virus scans are conducted by the ABS during and after file uploading. • Key systems within the ABS, including its internet gateway, server and network platform, are required to undergo formal and independent Information Security Registered Assessors Program (IRAP) assessment and accreditation.

	• The data will be stored in the ABS's Next-Generation Infrastructure (NGI) environment, which has been IRAP assessed and was accredited in line with ISM controls at the OFFICIAL:Sensitive level (although a majority of controls are implemented in accordance with the PROTECTED classification. • The data shared with the ABS is collected under the authority of the Census and Statistics Act 1905 and is afforded all the protections under that Act. This makes it a criminal offence for a current or former Statistician or officer to disclose the information unless it is for the purposes of that Act or released under section 13 of that Act. No information can be disclosed under section 13 in a manner that is likely to identify an individual. • ABS officers are also required to handle personal information in accordance with the Privacy Act 1988 and the Australian Privacy Principles, and to abide by the High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes. They are also bound by the Public Service Act 1999. All ABS staff sign a lifelong Undertaking of Fidelity and Secrecy under the Census Act and their data access (including access to the datasets subject to this PIA) is logged and monitored. • Data integration is undertaken by a dedicated ABS team in accordance with a 'separation principle' and within a secure environment. These procedures have been examined via this independent Privacy Impact Assessment. The separation principle means that no individual within the organisation can access both the identifying information used for linkage, such as names, addresses and dates of birth, and the analytical data which does

	not contain direct identifiers. This will involve the use of discrete functional roles: ○ Librarian: Prepares, standardises, and anonymises identifying data used for linkage. Typically, the linkage data are comprised of variables relating to name, address, date of birth, and sex or gender. Once this function is complete, the Agreement specifies that the ABS agrees to securely delete the original personal identifiers. ○ Linker: Links datasets using anonymised linkage data. ○ Assembler: Uses the linkage results to create linked analytical data. • The Administration Act creates offences for unauthorised obtaining of protected information, unauthorised making a record of, disclosure or use of protected information, soliciting disclosure of protected information, and offering to supply protected information. If the protected information provided by the Secretary under subparagraph 168(1)(b)(i) of the Administration Act is recorded, used or disclosed for a purpose other than the purposes of the ABS, the authorisation in paragraph 162(2)(e) will not apply and the offences in Div 2, Part 6 of the Administration Act may apply. • Personal identifiers will be provided separately for data linkage purposes only. Few select ABS officers have access to identifying data. Access is monitored, logged and audited. Individuals with access to identifying data do not have access to analytical data. • The Agreement provides that the ABS will destroy personal identifiers immediately following the creation of the PLIDA linkage results file and statistical linkage keys. The encrypted concordances will be quarantined securely in an environment

	separate to analytical data with strict access controls. • In the event of a data breach, the ABS is bound by its responsibilities under the Privacy Act. The Agreement also provides that in the event of a data breach during transmittal to or storage at the ABS, the ABS will notify the department immediately, and will include a departmental representative in the incident response team.
APP 12 – access to personal information If the department holds personal information about an individual, it must give the individual access to that information on request, unless an exception applies.	The department's Privacy Policy sets out procedures for individuals to access their personal information and nothing in the initiative will prevent the department from implementing those procedures, as required by APP 12. All Departmental staff involved in the project have completed mandatory Privacy training. All staff involved in the project are aware of their obligations under the Privacy Act.
APP 13 - correction of personal information The department must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.	The department's Privacy Policy sets out procedures for individuals to correct their personal information and nothing in the initiative will prevent the department from implementing those procedures, as required by APP 13.

Findings and recommendations

The below table sets out the privacy risks identified by the department and the strategies recommended to mitigate these risks. Where privacy risks are unable to be mitigated, the table explains why mitigation is not possible.

APP	Privacy risk	Mitigation strategy
10 – quality of personal information	Child Care Subsidy data is collected by Services Australia and stored in its EDW. The department extracts data from the EDW and relies on Services Australia to collect accurate, up to date and complete data.	The department will continue to engage with Services Australia regularly to monitor any issues with data quality. The department will continue to implement human data processing procedures to check the accuracy, contemporaneity and completeness of data accessed from the EDW before it is disclosed to the ABS under the Agreement. These human data processing procedures will be documented and reviewed.
APP 6	Risk that the secondary use or disclosure of personal information is not required or authorised by law.	The Agreement seeks to ensure that protected information is only disclosed to the ABS for the purposes of the ABS. Data sharing and use under the Agreement is limited to 'the purposes of the ABS … as specified in Annex 1' (p 3). The Agreement also provides that any on-disclosure of protected information 'is for a purpose of the ABS within its legislative framework' (p 5). However, the list of approved statistical purposes at Annex 1 includes data integration projects 'as approved by the CCA data delegate and the Australian Statistician (or their delegate)'; data linkage in PLIDA 'for future projects as agreed by the CCA data delegate and the Australian Statistician'; and data use in 'future statistical projects where these have been explicitly authorised by the CCA data delegate and the Australian Statistician' (p 11). The Agreement does not expressly confine the scope of any future agreement between the CCA data delegate and the Australian Statistician

		regarding matters in Annex 1 to purposes of the ABS. The department will obtain and document confirmation from the ABS, before recommending that the CCA data delegate gives any future agreement under Annex 1, that the ABS considers that the proposed use or disclosure is for the purposes of the ABS. The department has separately agreed with the ABS that if a proposed on-disclosure is not for a purpose of the ABS, the ABS will refer the data request to the department so consideration can be given to issuing a Public Interest Certificate (PIC) to authorise the disclosure.

Approval

I confirm that this PIA appropriately identifies all privacy risks associated with this initiative. and that adequate controls are in place or will be in place prior to the commencement of the initiative. for the protection of personal information.

I approve the mitigation strategies set out in this document and undertake to implement any mitigation strategies that are not already in place.

Approved by:

s22

Assistant Secretary, Data and Delivery Support Branch
Date: 20/05/2024

A copy of this PIA must be retained on file and sent to the Privacy Officer.

Document 2

Privacy Impact Assessment

Handling of data to support the Commonwealth Fraud Fusion Taskforce (FFT) and Australian Criminal Intelligence Commission (ACIC) FFT Intelligence Program

In accordance with the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (the Code), the Department of Education (the department) is undertaking a Privacy Impact Assessment (PIA) to determine whether this initiative is compliant with the *Privacy Act 1988* (Privacy Act), including the Australian Privacy Principles (APPs). This PIA will identify privacy risks associated with the initiative and counteractive steps that the department should take to avoid, minimise or mitigate identified privacy risks.

Project or initiative

Initiative description
This initiative entails the Department of Education's (the department's) handling of data and information to support the Services Australia and National Disability Insurance Agency (NDIA) led Commonwealth Fraud Fusion Taskforce (FFT) and Australian Criminal Intelligence Commission (ACIC) led FFT Intelligence Program, in support of the FFT and for ACIC's own purposes. **Background** **Commonwealth Fraud Fusion Taskforce** The Commonwealth-funded FFT is a multi-agency taskforce established in 2022 by the Commonwealth Government. It is a partnership between the NDIA, Services Australia and 15 other government agencies including the department, NDIS Quality and Safeguards Commission (NQSC), Australian Federal Police (AFP) and the ACIC. The FFT aims to work together to detect, disrupt and prevent fraud and Serious and Organised Crime (SOC) with an objective to improve payment integrity across government programs, including those managed by the department. It also seeks to reduce the opportunity for the

commission of fraud, non-compliance and financial losses, improving program integrity and in-turn enhancing government and community confidence in the public service.

The FFT will have a particular focus on the NDIS initially, with broader fraud and loss detection and prevention benefits for other government programs to follow. The FFT will assist all partner agencies by facilitating better information sharing and enabling an intelligence led approach to fraud guided by the FFT Intelligence Program.

The establishment of the FFT meets a key election commitment and is an important element of a Fraud and Integrity Strategy aimed at reducing loss to fraud, non-compliance and incorrect payments in the NDIS and other programs.

The FFT operates under the law and is governed by an ethics and human oversight framework. This makes sure the safety, wellbeing and privacy of participants in the NDIS and other Commonwealth programs is protected.

ACIC FFT Intelligence Program

The FFT intelligence program is led by ACIC to inform the work of the FFT through information and intelligence-sharing, leads generation and data analytics. This program involves the ACIC collecting criminal intelligence and analysing and crossmatching data from numerous sources (including but not limited to the department, NDIA, Services Australia, NQSC, Australian Taxation Office (ATO), AFP, Australian Securities and Investments Commission (ASIC), Australian Transaction Reports and Analysis Centre (AUSTRAC), Department of Health and Aged Care (DoHA), and Department of Employment and Workplace Relations (DEWR) to provide strategic and tactical intelligence advice to the FFT and its members to address the purpose and objectives of the FFT. Data collected in support of the FFT intelligence Program will be managed and held by the ACIC-led Fraud Fusion Centre.

The ACIC is not subject to the Privacy Act, however, its Information Handling Protocol states that it acts in accordance with the APPs 'wherever reasonably consistent with the effective performance of its statutory functions'.

The department's involvement in the FFT (the initiative)

The department has portfolio responsibility for supporting the Australian Government's commitment to affordable early childhood education and care (ECEC) and directly delivers several core operational functions to support Child Care Subsidy (CCS) financial integrity including Provider Approvals, Integrity Capability and Engagement, Compliance Operations, Fraud Investigations and Tactical Operations, Provider Audits, CCS Helpdesk and Strategic Communication.

The department has extensive CCS data and intelligence holdings to contribute to the key objectives of the FFT. s37(2)(b) s47E(d)

The NDIA and the ACIC engaged with the department prior to the formal commencement of the FFT to support its establishment. The department continues to work closely with NDIA and ACIC to support the objectives of the FFT and has enabled secondment of a subject matter expert staff member into the ACIC to establish governance arrangements and facilitate preliminary data sharing activities relating to the ECEC sector for the purposes of the FFT. These preliminary data sharing activities were authorised under the Public Interest Certificates (PICs) discussed below.

The initiative examined in this PIA is the department's handling of personal information for the purposes of its involvement in the FFT. The PIA does not consider the ACIC or member agencies' compliance with the APPs.

Data requested by the FFT

To date, the FFT has requested that the department provide a range of datasets (listed below) and the department anticipates providing additional data on request. Some information in these datasets is protected information under the Family Assistance Law (FAL). Legal mechanisms used to authorise the disclosure of protected information under the FAL are a combination of PICs and disclosures by the Secretary to their counterpart within the relevant agency through a disclosure instrument (Secretary disclosure instrument). More information is provided below.

Public Interest Certificates:

PICs have been given to authorise information and data sharing with the FFT for intelligence, criminal investigations and administrative purposes. Protected information disclosed under PICs remains protected information in the hands of the recipient, and may only be recorded, used or disclosed for the purpose described in the PIC. Partner agencies may not use or otherwise disclose the relevant information (unless aggregated and de-identified) for any other purpose, project or activity unless required or authorised by law. Written consent must be provided by the department prior to any further use, or disclosure by the receiving agency, and the department will consider whether the proposed use or disclosure is permitted under the FAL, including for the purposes of the PIC, or whether a new PIC or other legal arrangement is required.

The following PICs are currently in force:

- PIC 23-037 (supply) authorises disclosure of FAL protected information directly from the department to the ACIC (for its own purposes and the purposes of the FFT) and to other members of the FFT for relevant enforcement related activities. This includes for intelligence and criminal investigation purposes. See Attachment A.

- PIC 23-060 (supply) authorises disclosure of FAL protected information directly from the department to the AFP (for its own purposes and the purposes of the FFT) and to other members of the FFT for relevant enforcement related activities. This includes for intelligence and criminal investigation purposes. See Attachment B.

Title	Date Signed	Status	Notes
PIC 23-020 (Investigations)	24-Apr-23	Revoked	PIC covers disclosure to support investigations conducted by the FFT. Disclosure includes s37(2)(b) s47E(d)

			s37(2)(b) s47E(d) . This PIC was revoked on 30 October 2023 when the delegate signed PIC 23-037.
PIC 23-037 (supply)	30-Oct-23	In force	PIC revokes 23-020. New PIC clarifies the FFT structure and s37(2)(b) s47E(d) . New PIC also authorises the disclosure of protected information to the ACIC and other partner agencies comprising the FFT for enforcement related activities undertaken by ACIC or as part of the FFT.
PIC 23-060 (Supply)	14-Dec-23	In force	PIC covers disclosure to support investigations conducted by the FFT and AFP. Disclosure includes s37(2)(b) s47E(d) .

Secretary Disclosure Instruments:

The Secretary will provide authority through two instruments to disclose information and data sharing with the Chief Executive Officer of ACIC and the Commissioner of the AFP for the purposes of each respective agency. See Attachment C and Attachment D.

Information disclosed under this arrangement will remain protected under the Administration Act. The receiving agency may therefore only make a record of, disclose, or otherwise use the information in accordance with the purposes for disclosure set out in Attachment A of the instruments. As summarised in the table below, the purposes for disclosure set out in the instruments include that the receiving agency may use the information for the purposes of the agency, including any of the agency's statutorily defined functions. Accordingly, although the reason for the initial disclosure is for the purposes of the FFT, the receiving agency can use the information for any of that agency's purposes. s42(1)

The ACIC and AFP are responsible for seeking legal advice to ensure that their proposed use or disclosure of the information is consistent with those agencies' purposes.

Title	Date Signed	Status	Notes
Secretary Disclosure (to the ACIC)	TBC	Draft	Instrument covers disclosure of protected information for the purposes of the ACIC, including the FFT. Disclosure includes s37(2)(b) s47E(d)
Secretary Disclosure (to the AFP)	TBC	Draft	Instrument covers disclosure of protected information for the purposes of the AFP, including the FFT. Disclosure includes

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

The following specific data sets have been requested by the FFT in support of the FFT Intelligence Program, to enable data matching and correlation activities. As the FFT progresses, it is likely additional data sets will be requested.

Data to be disclosed under the 'ACIC – Secretary Disclosure Arrangement'

s37(2)(b) s47E(d)

Data to be disclosed under the 'AFP – Secretary Disclosure Arrangement'

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

Data to be disclosed to other Taskforce Agencies using the PIC arrangements

- Ad-hoc requests for information in relation to persons or entities of interest identified through FFT activities.

Where the FFT makes a request for data and information that is not encompassed under the Secretary disclosure instrument or PIC arrangements, the delegate will consider whether the disclosure is permitted under the FAL and Privacy Act, which may include making or amending the Secretary disclosure instruments or PICs to authorise the disclosure before it is made.

Purpose of sharing data with the FFT

The department will support the FFT to achieve its objective by sharing data and information relating to s37(2)(b) s47E(d) .

At a high level, disclosure of this information enables ACIC to perform its function under the *Australian Crime Commission Act 2002* (Cth) including the collection, correlation, analysis and dissemination of criminal information and intelligence to member agencies of the FFT.

Similarly, disclosure of this information enables AFP to perform its function under the *Australian Federal Police Act 1979* (AFP Act). In particular, the information supports the purpose described in section 8(1)(b) of the AFP Act: "the provision of police services in relation to laws of the Commonwealth; the safeguarding of Commonwealth interests…".

Specifically, the information will enable the FFT to s37(2)(b) s47E(d)

. This matching process will feed into s37(2)(b) s47E(d)

.

Governance arrangements

The data requested by the FFT is 'protected information' under Family Assistance Law (as defined in subsection 3(1) of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Cth) (the Administration Act) and contains personal information under the Privacy Act.

The Secretary of the department (or their delegate) may, if it is necessary in the public interest to do so in a particular case or class of cases, disclose protected information. In giving PICs, the Secretary (or their delegate) must act in accordance with the *Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018* (PIC Guidelines) issued by the Minister. Delegates of the Secretary have issued several PICs pertaining to FFT matters. The relevant delegate issued PIC CC 23-020 on 24 April 2023 to authorise the disclosure of protected information to the FFT for the purposes of the FFT under paragraph 168(1)(a) of the Administration Act and section 15 of the PIC Guidelines. This PIC has been subsequently revoked and replaced with new PICs, as outlined above, to authorise the disclosure of additional data for dual purposes.

There may be further updates to these PICs (or new PICs) made in response to requests for data and information by the FFT as the FFT evolves. This will ensure that the disclosure is authorised before any additional protected information is disclosed to the FFT or one of its members.

The use or disclosure of protected information that is also personal information to the FFT in accordance with these PICs is authorised by an Australian law for the purposes of the Privacy Act.

The Secretary of the department may disclose protected information to the Secretary of a Department of State of the Commonwealth or to the head of an authority of the Commonwealth for the purposes of that Department or authority, under section 168(1)(b)(i) of the *A New Tax System (Family Assistance) (Administration) Act 1999*. This is referred to above as a Secretary disclosure instrument. In disclosing information under paragraph 168(1)(b), the Secretary must act in accordance with guidelines (if any) from time to time in force under section 169. No such guidelines are in force. The disclosure of protected information that is also personal information under the Secretary disclosure instrument arrangement is authorised by an Australian law for the purposes of the Privacy Act.

The department has entered into a Memorandum of Understanding (MOU) with partner agencies of the FFT, which was signed by the Secretary of the department on 21 June 2023. See Attachment E. The MOU is currently being updated to incorporate additional partner agencies that have joined the FFT since it was enacted. The MOU will continue to be updated as new partner agencies join the FFT in future. The MOU formalises a collaborative and collegiate working relationship between the partner agencies, to effectively address the impact of fraud on the NDIS and other government programs and payments.

In addition, any disclosures of bulk data sets will include a covering letter that specifies further requirements relating to the controlled sharing of data under this initiative. See cover letter templates at Attachments F and G.

All departmental staff and contractors engaged in this initiative have completed privacy training and are aware of their obligations under the Privacy Act in relation to the handling of personal information. All Departmental staff engaged in this initiative hold a minimum of Negative Vetting Level 1 security clearance.

Key dates and timeframes
• The FFT was established in October 2022, following an election commitment made by the Albanese Government to 'get the NDIS back on track', noting extensive evidence of egregious fraud that involves complex criminal networks ripping off NDIS participants and Australian taxpayers. • The FFT will operate for a period of four years, commencing from 2022-23 until 2025-26. • While no timeframe has been provided for disclosure of the specified data sets, it is crucial to promptly disclose the information to ensure the FFT has ample opportunity to identify and address adverse behaviours in order to safeguard public revenue from fraudulent activities.

Stakeholders

The department will consult the following stakeholders.

Stakeholder name	Details of proposed consultation
Department of Education Privacy Team (Corporate and Information Law)	The department's privacy team will be provided with a copy of this PIA for review and will be consulted to further support the development of this assessment from a privacy law perspective.

The department has consulted the following stakeholders.

Stakeholder name	Response to consultation
Department of Education Early Childhood and Youth Legal Team ()	The department's Early Childhood and Youth Legal Team have provided advice on issues around the use and sharing of data under the Family Assistance Law and the development of the data sharing cover letters, PICs and Secretary disclosure instruments. The team is continuing to support the initiative with legal advice.
Australian Government Solicitor (AGS)	The AGS has provided advice supporting the development of this initiative. Specifically, the AGS has provided advice concerning the on-disclosure of protected information under the Family Assistance Law.
Intelligence Analytics Team, Financial Integrity Branch	The Intelligence Analytics team (IA) is continuing to engage and support the initiative, while also providing their insight into potential privacy issues. IA has drafted the PICs (in consultation with the Early Childhood and Youth Legal Team and AGS), this PIA and the data sharing cover letters to ensure adequate governance arrangements in support of the FFT.
Integrity Capability and Engagement Team	The Integrity Capability and Engagement (ICE) Team is supporting the initiative by facilitating engagement with key representatives of the FFT regarding governance, budget and the department's involvement with FFT activities.

Fraud Investigations and Tactical Operations Team	The Fraud Investigations and Tactical Operations Team has supported the initiative by providing resources to assist with the FFT operations where current and historical links to Child Care are identified.
ACIC Fraud Fusion Centre	The ACIC Fraud Fusion Centre are the main liaison point between the department and the FFT in regard to data acquisition, use and dissemination in support of the FFT intelligence program.
NDIA Taskforce Management Office (TMO)	The NDIA TMO are the liaison point between the department and the FFT in regard to administrative and governance arrangements for FFT operations. They are responsible for the preparation of the MOU and will facilitate review and finalisation of the sharing agreement.
NDIA	The NDIA are one of the main liaison points between the department and the FFT in regard to data acquisition, use and dissemination in support of the FFT targeted investigations.
AFP	The AFP form the operational arm of the wider FFT, supporting the Intelligence and Operations Committee Operational Working Group (IOC OWG). The AFP will use their data to s37(2)(b) s47E(d) complementing ACIC data matching projects.

Personal information flows

The department will handle personal information[1] in the initiative as follows.

a) The table below refers to information the department will disclose to the FFT.

Type of information	Collect	Use	Disclose	Store	Destroy	De-identify
s37(2)(b) s47E(d)	☑	☑	☑	☑	☑	☐
	☑	☑	☑	☑	☑	☐
	☑	☑	☑	☑	☑	☐

[1] 'Personal information' is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

s37(2)(b) s47E(d)						
	☑	☑	☑	☑	☑	☐
	☑	☑	☑	☑	☑	☐
	☑	☑	☑	☑	☑	☐

b) The table below refers to information the department will receive from the FFT.

Note: It is unclear as to what data may be shared by partner agencies as the focus of the FFT changes and expands from NDIS to other government payments and programs. The following reflects a logical estimate of potential disclosures to the department.

Type of information	Collect	Use	Disclose	Store	Destroy	De-identify
s37(2)(b) s47E(d)	☑	☑	☑	☑	☑	☐
	☑	☑	☑	☑	☑	☐

s37(2)(b) s47E(d)	☑	☑	☑	☑	☑	☐
	☑	☑	☑	☑	☑	☐

Collection	The department will collect personal information from FFT partner agencies for the purpose of data matching to s37(2)(b) s47E(d)
Use	The department will use CCS data to prepare it for disclosure to the FFT. This is data that the department already holds. The personal information to be disclosed to FFT members by the department is stored in the Services Australia Enterprise Data Warehouse (EDW) and is collected by Services Australia under the family assistance law on behalf of the department. The department has access to CCS data stored in the EDW through a shared services arrangement. In preparing the data, the department is required to extract the data from the Services Australia EDW and clean and transform it into tables, including deriving fields, applying rules and collating relevant data sets. The data will then be manually analysed to form valuable insights for Taskforce partner agencies. Some data may be extracted directly from the Child Care Subsidy IT system where it cannot be located in the EDW. The department will also prepare information stored in departmental holdings for disclosure. s37(2)(b) s47E(d) The FFT will use the data provided by the department to inform FFT operations and strategic insights, in accordance with the Secretary disclosure instrument or PIC and the data sharing requirements as outlined in the relevant cover letter. The s37(2)(b) s47E(d) will be used for data matching purposes to s37(2)(b) s47E(d) The analysis derived from the data matching process may also be used to contribute to

	s37(2)(b) s47E(d) The s37(2)(b) s47E(d) will be used for data matching purposes, to s37(2)(b) s47E(d) Documentation provided to the FFT may be used to initiate administrative proceedings of partner agencies, however this will only be actioned in close consultation with the department to ensure the use case is lawful. The data sharing cover letter outlines that the FFT 'must not use the relevant dataset for any other purpose, project or activity' unless required or authorised by law. Similarly, the department will use information provided by FFT partner agencies for data matching purposes to s37(2)(b) s47E(d) . Similar to above, the analysis derived from the data matching process may also be used to contribute to s37(2)(b) s47E(d) Documentation provided to the department by the FFT may be used to initiate administrative proceedings, however this will only be actioned in close consultation with the relevant partner agency to ensure appropriate visibility and that the information is used appropriately in administrative proceedings.
Disclosure	The department will disclose the personal information to the FFT for the purposes of supporting FFT objectives. The Secretary may disclose personal information to the ACIC and AFP under the Secretary Disclosure instruments. The department may also disclose personal information that is also protected information to FFT agencies under the PICs. Where consistent with the purposes specified in the Secretary disclosure instrument, which would include the FFT, on-disclosure of protected information held by the ACIC and AFP is authorised. These agencies are however bound by any restrictions imposed by their governing legislation and other regulatory frameworks in on-disclosing this information, which will remain protected under the Administration Act. The PICs currently in force do not permit the receiving agency to on-disclose protected information shared by the department under the PIC. The department will send relevant data and analysis via email to specific officers in the FFT. Where maximum size capacity is exceeded, the department will upload data to a secure file transfer portal that specific officers in the FFT can access and download data from. The FFT requests

access for specific officers who are then emailed an access link and one-time password. Once FFT officers access the link for the first time they are prompted to set individual unique passwords for their continued access. Once files are downloaded by the FFT, the department will immediately delete the data from the file transfer portal. Any files that are more than 30 days old will be automatically deleted from the file transfer portal.

Partner agencies of the FFT are as follows:

- Department of Education (The department)
- Australian Criminal Intelligence Commission (ACIC)
- NDIS Quality and Safeguards Commission (NQSC)
- National Disability Insurance Agency (NDIA)
- Services Australia
- Attorney-General's Department (AGD)
- Australian Federal Police (AFP)
- Australian Taxation Office (ATO)
- Commonwealth Director of Public Prosecutions (CDPP)
- Australian Securities & Investments Commission (ASIC)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Department of Health and Aged Care (DoHA)
- Department of Veterans' Affairs (DVA)
- Department of Employment and Workplace Relations (DEWR)
- Department of Social Services (DSS)
- Australian Skills Quality Authority (ASQA)
- Australian Charities and Not-for-Profits Commission (ACNC).

The data provided to the FFT will inform consultations, intelligence reports, s37(2)(b) s47E(d) for the purposes of the FFT. It is expected these reports will be provided to partner agencies identified as having vested interest or portfolio responsibility related to the subject matter. The FFT is responsible for ensuring that the outputs (including the reports) do not contain any personal information or protected information unless permitted by law.

The department may also disclose personal information relating to s37(2)(b) s47E(d)

A

	purpose of the FFT is to identify high risk entities s37(2)(b) s47E(d)
Storage	The FFT (including the department) must ensure the information disclosed is secure and cannot be accessed by unauthorised personnel. The department will store personal information disclosed by the FFT within the FFT SharePoint site, with appropriate access controls in place. Similarly, any data sets created by the department for the purposes of disclosure to the FFT will be saved within the FFT SharePoint site, with appropriate access controls in place. The information may also be stored in the Child Care Intelligence System (CCIS), which is an approved system for storing, analysing and reporting on intelligence related matters. A separate entity (file) in CCIS has been created for this information with appropriate access controls in place. Controls include limiting access to a particular 'user group' on a need-to-know basis. This is generally limited to Intelligence Analysts and Fraud Control Officers in the Intelligence Analytics team within the Financial Integrity Branch. A limited number of staff within the Integrity Capability and Engagement Team and Fraud Investigations and Tactical Operations team may also be required to access FFT information in the course of their duties. If these circumstances arise, access to isolated case information will be provided to relevant staff as required. Further information relating to their role in the initiative is outlined on Page 6, in the 'Stakeholders' section. Personal information provided to the FFT by the department will be extracted from the sender email or the department's file transfer portal and stored fully or partly on ACIC's IT network.
Destruction	Files will be automatically deleted from the file transfer portal after 30 days. Personal information will be managed in accordance with the *Archives Act 1983*.
De-identification	The s37(2)(b) s47E(d) will not be de-identified for the purposes of the FFT and will include personal information. De-identifying individuals is not reasonably practical for FFT purposes as it would render the data unusable.

Analysis of APP compliance

The below table analyses the compliance of the initiative against each APP.

APP	Analysis

APP 1 – open and transparent management of personal information The APP entity must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way.	The department has a Privacy Policy in place to ensure it manages personal information in an open and transparent way, consistent with APP 1. The disclosure of data to the FFT is also governed by a MOU, data sharing requirements (outlined in a cover letter that accompanies each bulk data set), secretary disclosure instruments, PICs 23-037 and 23-060 and any subsequent instruments or PICs, which outline the data that will be transferred to the FFT and the expectations for data handling within this initiative. The existence of a MOU, data sharing cover letter, Secretary disclosure instruments and PICs promotes openness and transparency about how personal and protected information will be handled for this specific initiative. The department has also undertaken this PIA as part of its implementation of practices, procedures and systems that comply with the APPs, as required under APP 1.2. The department understands that each FFT member agency will conduct its own PIA if required. The department will also make any necessary amendments to the Secretary disclosure instruments, PICs and this PIA as the FFT progresses to ensure the department is managing the personal and protected information relating to this initiative in an open and transparent way.
APP 2 – anonymity and pseudonymity Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter, unless an exception applies.	It is not generally practicable for individuals to deal with the department anonymously or using a pseudonym in relation to the administration of the CCS. For the purposes of this initiative, data cannot be anonymised (including s37(2)(b) s47E(d)) because that would prevent the FFT from s37(2)(b) s47E(d)
APP 3 – collection of solicited personal information	The department is a member of the FFT and the personal information collected by the department from FFT members is reasonably necessary for the department's functions as a

Any personal information collected (other than sensitive information) must be reasonably necessary for or directly related to one or more of the department's functions or activities. The department must not collect sensitive information[2] about an individual unless one of the exceptions listed in APP 3.3 or APP 3.4 applies, such as if the individual consents and the information is reasonably necessary for or directly related to one of more of the department's functions or activities. Personal information can only be collected by lawful and fair means. Personal information about an individual must only be collected from the individual unless one of the exceptions in APP 3.6 applies.	FFT member and its activities related to promoting integrity in the child care sector. The personal information, including sensitive information, being collected by the department from partner agencies as part of this initiative is necessary to enable data matching activities to identify s37(2)(b) s47E(d) . There are no provisions under the FAL which prevent the department from "collecting" information from other Commonwealth entities, as long as the information is disclosed in a manner consistent with the relevant agency's legislation. The MOU provides that information sharing for the FFT must comply with the Privacy Act and relevant secrecy laws. In particular, it states that 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 (cl 14(4)). Similarly, the FFC Data Governance Plan states that 'the contributing agency is responsible for articulating any use, handling, and disclosure restrictions to the ACIC'. The department expects that FFT members will disclose information to the department under the disclosing agency's secrecy provisions. The department anticipates receiving a notice from the disclosing agency, similar to the approach taken in the letter from the NDIS to the ACIC, which outlined the legal basis for disclosing the relevant datasets and applicable limitations. In circumstances where the disclosure of personal information (including sensitive information) is authorised by the secrecy provisions in the disclosing agency's legislation, the department's collection of sensitive information about an individual will be

[2] Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

	authorised by law for the purposes of APP 3.4(a). The department will collect personal information about individuals from the FFT rather than from the individuals concerned. The department will rely on the following exceptions in APP 3.6: • the department is authorised by law to collect the information from the FFT member (for example, under a PIC issued by the originating agency) (APP 3.6(a)(ii)); or • it is unreasonable or impracticable to obtain the information from the individual (APP 3.6(b)). The APP Guidelines acknowledge that the exception in APP 3.6(b) may be available in relation to collection by a law enforcement agency of personal information about an individual who is under investigation, where the collection of the information from the individual may jeopardise the investigation.
APP 4 – dealing with unsolicited personal information Where an APP entity receives unsolicited personal information,[3] it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the APP entity must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.	As the Taskforce has extensive data governance arrangements in place, it is unlikely that the Department will receive unsolicited personal information. In the event that the department does receive unsolicited personal information, for example, if it is inadvertently provided with personal information intended for another FFT member agency, the department will consider whether it may collect the personal information under APP 3 (and if so, handle the personal information in accordance with the APPs). If the department is not authorised to collect the personal information under APP 3, the

[3] Personal information that the department did not solicit or ask for from individuals.

	department will handle the information in accordance with the *Archives Act 1983* or APP 4.3 as applicable.
APP 5 – notification of the collection of personal information Where the department collects personal information about an individual, it must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of the matters listed in APP 5.2. The department must provide notification before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection. The matters listed in APP 5.2 include: (a) the department's and, if relevant, its contracted service provider's identity and contact details (b) the facts and circumstances of collection (c) whether the collection is required or authorised by law (d) the purposes of collection (e) the consequences if personal information is not collected (f) the department's and, if relevant, it's contracted service provider's usual disclosures of personal information of the kind collected (g)–(h) information about the department's privacy policy (i)-(j) whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located. A privacy statement template is available on the intranet.	**Notice of collection** APP 5 requires the department to take 'such steps (if any) as are reasonable in the circumstances' to notify individuals of the matters in APP 5.2. The APP Guidelines explain that the steps required will depend on matters such as the sensitivity of the information and the possible adverse consequences for an individual. Both these factors may be relevant to personal information collected by the department in connection with the FFT. However, the APP Guidelines provide the following relevant examples of when not taking any steps may be reasonable: • notification may pose a serious threat to the life, health or safety of an individual or pose a threat to public health or safety, for example, a law enforcement agency obtaining personal information from a confidential source for the purpose of an investigation. • notification may jeopardise the purpose of collection or the integrity of the personal information collected and there is a clear public interest in the purpose of collection, for example, a law enforcement agency undertaking lawful covert surveillance of an individual in connection with a criminal investigation. The department considers that notifying persons of interest about the collection of their personal information may compromise the

	work of the FFT. However, if the department is collecting large datasets it may not be the case that notifying this cohort would 'tip-off' a person of interest. There may also be an argument that a collection notice would promote the purposes of the FFT by warning that fraud is being actively investigated. Individuals are broadly on notice that the department may collect their personal information from other departments. For example, the Child Care Subsidy privacy notice for customers states that Services Australia can share information with the Department and 'other parties where the release is authorised by law, including for the purpose of … investigations'. Information about the Fraud Fusion Taskforce is publicly available, including on the NDIS website. The NDIS Fraud Strategy Statement states that the NDIS uses 'information and data' to detect fraud and that it works with other Commonwealth agencies to address fraud. In addition, the department's privacy policy relevantly states that the department collects personal information for purposes including 'preventing, detecting, investigating or dealing with corruption, misconduct and fraud, cyber-attacks against the Commonwealth, or other unlawful activity relating to the Commonwealth'. However, the privacy policy also states that the department will generally provide a privacy notice when it collects personal information, and the APP Guidelines note that a privacy notice under APP 5 is distinct from privacy policy requirements. **Notice of usual disclosures** The requirement in APP 5.2(f) relates to notifying individuals of the recipients or types of recipients to which the department 'usually discloses' personal information of the kind it collects. The APP Guidelines note that a 'usual' disclosure is one that occurs regularly, under an agreed arrangement, or that can reasonably be predicted or anticipated'.

	The FFT was established in 2022 and is anticipated to run for 4 years until June 2026. To the extent that the department will 'usually disclose' personal information to FFT members, the department's privacy policy relevantly states that the department discloses personal information for purposes including 'data sharing with other Australian Government agencies' and 'preventing, detecting, investigating or dealing with corruption, misconduct and fraud … or other unlawful activity relating to the Commonwealth'. The department should consider whether a specific privacy notice is required to ensure that individuals are sufficiently notified of any 'usual disclosures' to FFT members. Alternatively, the department should consider updating the department's privacy policy to specifically refer to the FFT in the relevant sections of part 2 of the policy. The department should also consider including details about its involvement with the FFT on the department's website in a similar fashion to the information that is contained on the NDIS website or Services Australia's website .
APP 6 – Use or disclosure of personal information The department can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. Exceptions permitting use or disclosure for a secondary purpose include, for example, where: (a) the individual consents to the use or disclosure (b) the individual would reasonably expect the use or disclosure, and the secondary purpose is related to the primary purpose or, in the case of sensitive information, directly related to the primary purpose (c) the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order.	CCS data, including any personal information, already held by the department was originally collected for the primary purpose of administering the CCS. Therefore, disclosing this personal information to the FFT to s37(2)(b) s47E(d) will involve using and disclosing the information for a different/secondary purpose. However, the department's use and disclosure of personal information for a secondary purpose is consistent with APP 6.1 because the use or disclosure of the personal information is authorised by an Australian law (APP 6.2(b)), namely the disclosures by the Secretary to the Agency Heads of the ACIC/AFP made in accordance with paragraph 168(1)(b)(i) of the Administration Act (Secretary disclosure instruments) and PICs 23-037 and 23-060,

	made under section 168(1)(a) of the Administration Act and section 9 of the PIC Guidelines. Where the department collects personal information from the FFT for the purposes of investigating and taking administrative action under the Family Assistance Law, its use of the information to do those things will be consistent with the primary purpose of collection.
APP 7 – Direct Marketing An organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies, such as where the individual has consented.	The department is not one of the agencies specified under section 7A of the Privacy Act. Therefore, APP 7 does not apply to the department.
APP 8 – cross-border disclosure of personal information Before the department discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent. If the department discloses personal information to an overseas recipient, it is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (see s 16C of the Privacy Act). **Publication of personal information on a public facing website could constitute a cross-border disclosure of personal information where that website can be accessed by people located overseas.**	Personal information is not going to be disclosed to an overseas recipient. As personal information is not going to be disclosed overseas, APP 8 is not relevant to this initiative.
APP 9 – adoption, use or disclose of government related identifiers An organisation must not adopt, use or disclose a government related identifier of an individual as its own identifier of the individual unless an exception applies. APP 9 generally applies only to organisations and does not in most instances apply to the department. However, separate legislative restrictions apply to the use of government related identifiers.	The department is not one of the agencies specified under section 7A of the Privacy Act. Therefore, APP 9 does not apply to the department.

APP 10 – quality of personal information
 	
The department must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. The department must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.
	The following steps will be taken to ensure that the personal information the department handles in this initiative is accurate, up-to-date, complete and relevant, having regard to the purpose for which it is being handled.
	
	Data the department will <u>disclose</u> to the FFT:
	
	• The department considers that the data requested by the FFT will support analysis and reporting of high-risk entities for the purposes of the FFT.
	• The CCS data disclosed by the department will be drawn from the Services Australia EDW. Where possible it will be subjected to quality assurance processes to ensure accuracy, including peer reviews of code used to extract the data.
	• Data is also manually reviewed by the department and, where possible, quality assured before it is transferred to the FFT, including high level analysis to ensure the data is consistent with other departmental holdings. For example, extracts may be cross checked against s37(2)(b) s47E(d)
	
	• Spot checks are also implemented to ensure data extracts are complete and relate to the correct entity. Areas of the department also review the data for compliance and integrity purposes.
	• Data which may take time to settle is only provided for time periods where the department has a high level of confidence that there is a reasonable level of stability in the data.
	• The department will have an open channel of communication with the receiving agency to:
	  ○ understand the data properties
	  ○ clarify any uncertainties, and
	  ○ address any issues identified with data quality.
	• Issues or discrepancies encountered will be documented for future reference and resolution if required before any action is taken.

	• The parties' expectations regarding data quality are set out in the data sharing cover letter, or within the body of the email in which the information is disclosed.
	
	Data the department will receive from the FFT:
	
	• The department considers that the data received by the FFT will support analysis and reporting of high-risk entities for the purposes of the FFT.
	• Data will be reviewed to identify any discrepancies or potential errors. E.g. missing data, inconsistencies, mis-matches with common fields.
	• Cross referencing with previous data sets disclosed by the relevant agency will be conducted to ensure consistency.
	• The department will have an open channel of communication with the sending agency to:
	  ○ understand the data properties
	  ○ clarify any uncertainties, and
	  ○ address any issues identified with data quality.
	• Issues or discrepancies encountered will be documented for future reference and resolution if required before any action is taken.
	
	The department strives to diligently quality assure data in line with the steps above, yet acknowledges that despite its best efforts, mismatches and errors may occur, particularly when information collected from individuals is inherently incorrect, misleading and beyond our control.

APP 11 – security of personal information An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that the	The following steps have been taken to ensure that the personal information the department handled in this initiative to protect the information from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure: • The PICs currently in place (PIC CC 23-037 and CC 23-060) only authorise relevant staff of the department and the FFT to disclose and receive the information.

information is de-identified, unless an exception applies.	• Data to be disclosed to the FFT is held by the department in a secure SharePoint site and is only accessible by a limited number of officers who require access in the Intelligence Analytics team and Integrity Capability and Engagement team. • When data is transferred to the FFT, this is done through a secure electronic environment (where attachments exceed standard size limit) to which only a limited number of officers in the FFT have access. The FFT requests access for specific officers who are then emailed an access link and one-time password. Once FFT officers access the link for the first time they are prompted to set individual unique passwords for their continued access. The department maintains a list of all individuals who have access. • Access to the department's systems require two-factor authentication methods, with data being held on Australian secure servers. • When data is transferred to the FFT, that meets minimum size limits, this is sent through email to specific contacts from registered member agencies of the FFT. • All involved departmental officers have completed mandatory privacy training and hold a minimum of a Negative Vetting Level 1 security clearance and can only access information on a 'need to know' basis. • The Fraud Fusion Centre data governance plan requires all partner agencies to comply with security policies, guidelines and advisories in the relevant Protective Security Management Framework, the Australian Government Protective Security Policy Framework and Australian Government Information Security Manual for the purposes of the FFT. Partner agencies are to notify ACIC in writing as soon as possible if any breaches occur. • The data sharing cover letter limits the use of the personal information and prohibits the publication or further

	disclosure of personal information by the FFT unless permitted by law. Data disclosed by the Secretary to the CEO of ACIC and the Commissioner of the AFP may be on-disclosed or otherwise used if consistent with those agencies' purposes. The receiving agency is responsible for seeking legal advice to ensure their proposed use or disclosure of the information is consistent with these purposes, acknowledging that the information remains protected under the FAL. • Unless required or authorised by law, the FFT must no longer access, use, share or release (or otherwise disclose) the data the department shared with them after the expiry or termination of the FFT. The ACIC and AFP may access and use the data the department shared with them for their own purposes past the termination date as long as it is consistent with those agencies' purposes.
APP 12 – access to personal information If the department holds personal information about an individual, it must give the individual access to that information on request, unless an exception applies.	The department's Privacy Policy and Guide to Accessing and Correcting Personal Information sets out procedures for individuals to access their personal information. The department's procedures recognise that APP 12 does not require the department to give access where the department is required or authorised by law to refuse to give access. The MOU sets out consultation requirements that may be relevant to an access request for personal information the department obtained from the FFT, including consulting with the originating agency and taking 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 (see cl 14(9)). Nothing in the MOU will prevent the department from implementing its procedures relating to access to personal information, as required by APP 12.

APP 13 – Correction of personal information The department must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.	The department's Privacy Policy and Guide to Accessing and Correcting Personal Information sets out procedures for individuals to correct their personal information. While the department would need to consider any consultation requirements under the MOU in the event of a correction request relating to information obtained from the FFT, this would not prevent the department from implementing its access procedures as required by APP 13, noting that these procedures provide that the department may refuse to correct personal information if it is not satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading.

Findings and recommendations

The below table sets out the privacy risks identified by the department and the strategies recommended to mitigate these risks. Where privacy risks are unable to be mitigated, the table explains why mitigation is not possible.

APP	Privacy risk	Mitigation strategy
APP 3 – collection of personal information	There is a risk that the department's collection of personal information will not comply with APP 3.3 in all cases.	The department should ensure that it confirms with the originating FFT member, before collecting personal information, that the FFT member is authorised by law to disclose the specific information to the department. This is important to ensure that the department's collection of any sensitive information, as well as the department's indirect collection of personal information, is authorised and that the department complies with any applicable secrecy provisions.
APP 5 – notification of the collection of personal information	There is a risk that individuals are not sufficiently informed of APP 5 matters in relation to personal information handled by the department in relation to the FFT.	The department should consider whether any additional steps are reasonable in the circumstances to notify individuals (or otherwise ensure awareness of) the relevant APP 5 matters. Further steps may not be required if the additional steps would compromise the purpose of the collection, for example, by 'tipping-off' persons of interest. For the avoidance of doubt about whether individuals have been adequately informed about the handling of their personal information in connection with the FFT, the department may wish to engage with the NDIA and Services Australia (as the joint lead agencies of the FFT) about whether a privacy statement for the FFT is already available or if this is required. Alternatively, the department could consider developing a specific privacy notice (for example, to be displayed on an appropriate page of its website) advising that information collected under the FAL may be disclosed to FFT members for the purposes of the FFT.

		At a minimum, the department should consider including general information about the FFT and the department's involvement, similarly to the information contained on the NDIS website or Services Australia's website about the FFT. The department could also consider amending the department's privacy policy to specifically refer to the handling of personal information for the purposes of the FFT.
APP 6 – Use or disclosure of personal information	There is a risk that the use or disclosure of personal information is not authorised, particularly in relation to future requests not covered by the existing PICs.	The department should establish a process for ensuring that all data transfers to the FFT containing personal information and / or protected information are authorised in advance of the transfer. The department will carefully consider any requests for additional data from the FFT and, before providing this data, ensure that: • the additional data is protected information; • if applicable, the PICs are updated (or revoked and replaced) to cover the additional protected information to be disclosed, including in circumstances where new agencies become members of the FFT and request protected information; • the updates to the PICs are consistent with the Family Assistance Law, specifically the Administration Act and the PIC Guidelines; • if applicable, the Secretary's disclosure instruments are varied to cover the additional protected information to be disclosed, • the variations to the Secretary's disclosure instruments are consistent with the Family Assistance Law, and

		• the relevant data sharing cover letter is updated if necessary. The department should also consider whether it is practicable to disclose de-identified information on a case-by-case basis. If the FFT requests additional protected information that is not supported by the PIC Guidelines or the Secretary disclosure instruments, the department will need to consider whether there is another basis for disclosure under the Administration Act. If the FFT requests additional personal information that is not protected information, the department will need to identify another basis for disclosure under APP 6.
APP 6 – Use or disclosure of personal information	There is a risk that the personal information disclosed for a particular purpose is disclosed/used for broader purposes.	Under the Secretary disclosure instruments, information may only be disclosed for the prescribed purpose (i.e., for the purposes of the receiving agency). The department will confirm that any subsequent requests for additional information from the ACIC and AFP are for the purposes of that agency. The PICs only permit disclosure for the prescribed purpose (i.e. for the purposes of the FFT). The department will confirm that any subsequent requests for additional information from FFT member agencies, other than the ACIC and AFP are for the purposes of the initiative.
APP 1 and 11 – security of personal information	There is potential for data matching to pose a risk to an individual's privacy.	The department should consider whether the 'Guidelines on data matching in Australian Government administration' apply to the data matching activities in this project. These Guidelines, which are issued under s 28(1)(a) of the Privacy Act, are voluntary but represent the OAIC's view on best practice with respect to undertaking data matching activities. The OAIC may take the Guidelines into

		account when assessing whether an agency has complied with the APPs. If the department considers they do apply, the department should consult with the other FFT agencies to confirm that view and to establish which agency is best placed to lead that work.
APP 11 – security of personal information	The use of email presents the risk of inadvertent disclosure of personal information	OAIC's most recent Notifiable Data Breaches Report (published in September 2023) found that a significant proportion of data breaches caused by human error resulted from emails sent to the wrong recipient. The department should consider whether all transfers of personal information could be done via the secure file transfer portal. If this is not practicable, the department should adopt a 'shoulder check' procedure before disclosing personal information to the FFT. This involves a colleague confirming that an email contains the correct address, content and attachments before it is sent externally.

Attachments

Attachment A: Public Interest Certificate - ACIC Supply (IN FORCE) (PIC CC 23-037)

Attachment B: Public Interest Certificate - AFP Supply (IN FORCE) (PIC CC 23-060)

Attachment C: Secretary Disclosure Instrument (to the ACIC) (LEX 50311)

Attachment D: Secretary Disclosure Instrument (to the AFP) (LEX 50311)

Attachment E: Memorandum of Understanding (DRAFT)

Attachment F: Data Sharing Cover Letter Template (PIC disclosure)

Attachment G: Data Sharing Cover Letter Template (Secretary disclosure)

Approval

I confirm that this PIA appropriately identifies all privacy risks associated with this initiative. and that adequate controls are in place or will be in place prior to the commencement of the initiative. for the protection of personal information.

I approve the mitigation strategies set out in this document and undertake to implement any mitigation strategies that are not already in place.

Approved by:

s22

Assistant Secretary, Financial Integrity Branch

Date: 27/05/2024

A copy of this PIA must be retained on file and sent to the Privacy Officer.

Australian Government
Department of Education

PIC CC 23-037

A New Tax System (Family Assistance) (Administration) Act 1999

Public Interest Certificate

I, s22 , Intelligence Analytics, Early Childhood and Youth Group of the Department of Education (the department), make this instrument under paragraph 168(1)(a) of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Admin Act).

Dated 24 May 2024

s22

Disclosure of information in the public interest

1 Commencement

This instrument commences on the day it is signed.

2 Revocation

The public interest certificate 23-020 issued by me under paragraph 168(1)(a) of the Admin Act on 24 April 2023 is revoked.

3 Certification

In accordance with:

(a) paragraph 168(1)(a) of the Admin Act; and

(b) the purpose for disclosure provided for in section 9 of the *Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018*;

I certify that in the case described in section 4, it is necessary in the public interest to disclose the information mentioned in section 6 to a person mentioned in section 7 for the purpose mentioned in section 5.

4 Case

Where the disclosure of the information will facilitate the carrying out of an enforcement related activity.

5 Purpose for which information may be disclosed

The purpose for which information may be disclosed is to facilitate an enforcement related activity which is or will be undertaken as part of the Fraud Fusion Taskforce or by the Australian Criminal Intelligence Commission.

6 Information able to be disclosed

a) Information relating to s37(2)(b) s47E(d)

The following information, may be disclosed:
s37(2)(b) s47E(d)

b) Information relating to individuals

The following information about s37(2)(b) s47E(d)
mentioned in section 6(a) may be disclosed:

s37(2)(b) s47E(d)

c) Information to the effect that there is no information held by the department about any of the s37(2)(b) s47E(d) listed in this section, may be disclosed.

7 Recipients of information

The information identified in section 6 may be disclosed to:

(a) any person who holds an office in or is employed in, or is seconded to, a member agency or body in the Fraud Fusion Taskforce who from time to time is responsible for facilitating the matters mentioned at section 5; and

(b) any person who holds an office in or is employed in, or is seconded to, the Australian Criminal Intelligence Commission who from time to time is responsible for facilitating the matters mentioned at section 5.

8 Persons authorised to disclose the information

An officer of the department is authorised to disclose the information held by the department mentioned in section 6.

9 Definitions

In this instrument, terms used have the same meaning that they have in the Admin Act.

Enforcement related activity has the meaning that it has in the *Privacy Act 1988*.

Member agency or body of the Fraud Fusion Taskforce means any of the following:

- Department of Education (DoE)
- National Disability Insurance Agency (NDIA)
- Services Australia
- Australian Criminal Intelligence Commission (ACIC)
- NDIS Quality and Safeguards Commission (NQSC)
- Attorney-General's Department (AGD)
- Australian Federal Police (AFP)
- Australian Tax Office (ATO)
- Commonwealth Director of Public Prosecutions (CDPP)
- Australian Securities & Investments Commission (ASIC)

- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Department of Health and Aged Care (DoHA)
- Department of Veterans' Affairs (DVA)
- Department of Employment and Workplace Relations (DEWR)
- Department of Social Services (DSS)
- Australian Skills Quality Authority (ASQA)
- Australian Charities and Not-for-Profits Commission (ACNC)
- Any other agency or body which joins the Fraud Fusion Taskforce subsequent to the making of this authorisation.

s37(2)(b) s47E(d)

10 Note

Please note that information disclosed in accordance with this public interest certificate is 'protected information' as defined in 3(1) of the Admin Act. The unauthorised use or on-disclosure of this information (including the on-disclosure of the information between member agencies or bodies of the Fraud Fusion Taskforce in circumstances where this is not authorised under the Admin Act) can be an offence.

Australian Government
Department of Education

PIC CC 23-060

A New Tax System (Family Assistance) (Administration) Act

1999 **Public Interest Certificate**

I, s22 Intelligence Analytics, Early Childhood and Youth Group of the Department of Education (the department), make this instrument under paragraph 168(1)(a) of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Admin Act).

Dated 24 May 2024
s22

Disclosure of information in the public interest

1 Commencement

This instrument commences on the day it is signed.

2 Certification

In accordance with:

(a) paragraph 168(1)(a) of the Admin Act; and

(b) section 9 of the *Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018;*

I certify that in the case described in section 3, it is necessary in the public interest to disclose the information mentioned in section 5 to a person mentioned in section 6 for the purpose mentioned in section 4.

3 Case

Where the disclosure of the information will facilitate the carrying out of an enforcement related activity.

4 Purpose for which information may be disclosed

The purpose for which information may be disclosed is to facilitate an enforcement related activity which is or will be undertaken as part of the Fraud Fusion Taskforce or by the Australian Federal Police.

5 Information able to be disclosed

The information to be disclosed for the purpose described in section 4 above includes the following information held by the department, relating to:

a) Information relating to

s37(2)(b) s47E(d)

6 Recipients of information

The information identified in section 5 may be disclosed to:

(a) any person who holds an office in or is employed in, or is seconded to, a member agency or body in the Fraud Fusion Taskforce who from time to time is responsible for facilitating the matters mentioned at section 4; and

(b) any person who holds an office in or is employed in, or is seconded to, the Australian Federal Police who from time to time is responsible for facilitating the matters mentioned at section 4.

7 Persons authorised to disclose the protected information

An officer of the department is authorised to disclose the information held by the department mentioned in section 5.

8 Interpretation

(a) In this instrument, terms used have the same meaning that they have in the Admin Act.

(b) In this instrument, unless the contrary intention appears:

Enforcement related activity has the meaning that it has in the *Privacy Act 1988.*

Member agency or body of the Fraud Fusion Taskforce means any of the following:

(a) Department of Education (DE)
(b) National Disability Insurance Agency (NDIA)
(c) Services Australia
(d) Australian Criminal Intelligence Commission (ACIC)
(e) NDIS Quality and Safeguards Commission (NQSC)
(f) Attorney-General's Department (AGD)
(g) Australian Federal Police (AFP)
(h) Australian Tax Office (ATO)
(i) Commonwealth Director of Public Prosecutions (CDPP)

(j) Australian Securities & Investments Commission (ASIC)
(k) Australian Transaction Reports and Analysis Centre (AUSTRAC)
(l) Department of Health and Aged Care (DoHA)
(m) Department of Veterans' Affairs (DVA)
(n) Department of Employment and Workplace Relations (DEWR)
(o) Department of Social Services (DSS)
(p) Australian Skills Quality Authority (ASQA)
(q) Australian Charities and Not-for-Profits Commission (ACNC)
(r) Any other agency or body which joins the Fraud Fusion Taskforce subsequent to the making of this authorisation.

s37(2)(b) s47E(d)

9 **Note**

Please note that information disclosed in accordance with this public interest certificate is 'protected information' as defined in 3(1) of the Admin Act. The unauthorised use or on-disclosure of this information (including the on-disclosure of the information between member agencies or bodies of the Fraud Fusion Taskforce in circumstances where this is not authorised under the Admin Act) can be an offence.

OFFICIAL: Sensitive
Legal Privilege

Australian Government
Department of Education

Your Ref
Our Ref LEX 50311

Secretary
Mr Tony Cook PSM

Ms Heather Cook
Chief Executive Officer
Australian Criminal Intelligence Commission
GPO Box 1936
CANBERRA CITY ACT 2601

Dear Ms Cook

Disclosure of protected information for the purposes of the Fraud Fusion Taskforce

Through ongoing correspondence with the Department of Education's (department) s22 , the Australian Criminal Intelligence Commission (ACIC) has requested the disclosure of protected information for the purposes of the ACIC, including as they relate to the Fraud Fusion Taskforce.

I have authorised the disclosure of protected information to you as Chief Executive Officer of the ACIC for the purposes of the ACIC (**Attachment A**).

This information remains protected information in the ACIC's hands and may only be used for the purposes for which it was disclosed. To help the ACIC's officers understand their obligations, I enclose a summary of legal advice given by the Australian Government Solicitor (**Attachment B**). Going forward, it will be the ACIC's responsibility to safeguard the information and ensure it is only used, recorded and disclosed for the purposes of the ACIC.

If you require any further assistance in this matter, please contact s22

Yours sincerely

[insert signature]

Tony Cook

[insert date]

A New Tax System (Family Assistance) (Administration) (Release of Protected Information) (ACIC) Authorisation 2024

I, TONY COOK, Secretary of the Department of Education, acting under subparagraph 168(1)(b)(i) of the *A New Tax System (Family Assistance) (Administration) Act 1999*, authorise the disclosure of the protected information mentioned in Schedule 1 to the head of the Australian Criminal Intelligence Commission (ACIC) for the purposes of that authority.

Dated [Day Month Year]

[Insert signature]

---

1. Context

(1) The Department of Education (department) and the ACIC are members of the Fraud Fusion Taskforce (FFT).

(2) The FFT is a partnership between the NDIA, Services Australia and 15 other government agencies (including the department and the ACIC), which aims to detect, disrupt and prevent fraud and Serious and Organised Crime (SOC) with an objective to improve payment integrity across government programs.

(3) The department is providing information to the ACIC that is relevant to the ACIC's role in providing strategic and tactical intelligence advice as part of the Fraud Fusion Taskforce (FFT).

(4) The ACIC will also be able to use that information for any purpose of the ACIC, including but not limited to the purpose described in subsection (3).

2. Interpretation

(1) In this instrument, terms used have the same meaning that they have in the *A New Tax System (Family Assistance) (Administration) Act 1999*.

(2) In this instrument, unless the contrary intention appears:

Member agency or body of the Fraud Fusion Taskforce means any of the following:

(a) Department of Education (DE)
(b) National Disability Insurance Agency (NDIA)

(c) Services Australia
(d) Australian Criminal Intelligence Commission (ACIC)
(e) NDIS Quality and Safeguards Commission (NQSC)
(f) Attorney-General's Department (AGD)
(g) Australian Federal Police (AFP)
(h) Australian Tax Office (ATO)
(i) Commonwealth Director of Public Prosecutions (CDPP)
(j) Australian Securities & Investments Commission (ASIC)
(k) Australian Transaction Reports and Analysis Centre (AUSTRAC)
(l) Department of Health and Aged Care (DoHA)
(m) Department of Veterans' Affairs (DVA)
(n) Department of Employment and Workplace Relations (DEWR)
(o) Department of Social Services (DSS).
(p) Australian Skills Quality Authority (ASQA)
(q) Australian Charities and Not-for-Profits Commission (ACNC)
(r) Any other agency or body which joins the Fraud Fusion Taskforce subsequent to the making of this authorisation.

s37(2)(b) s47E(d)

3. Purpose of initial disclosure

(1) I am satisfied that the initial disclosure to the ACIC described in subsection 1(3) is for the purposes of the ACIC. Those purposes are described in the *Australian Crime Commission Act 2002* (ACC Act). In particular, the information supports the purpose described in section 7A of the ACC Act: "to collect, correlate, analyse and disseminate criminal information and intelligence…".

(2) Subsection (1) does not, by implication, limit the purposes for which information is disclosed under this instrument, being "for the purposes of that authority".

Schedule 1— Information able to be disclosed

The following information may be disclosed:

1. Information about providers

s37(2)(b) s47E(d)

2. Information relating to individuals

s37(2)(b) s47E(d)

3. Information not held

Information to the effect that there is no information held by the department about any of the Providers, services or individuals listed in this section, may be disclosed.

Legal Advice

The following summary of legal advice given by the Australian Government Solicitor is provided pursuant to the *Legal Services Directions 2017*. Legal privilege is not waived.

s42(1)

The agency receiving protected information is responsible for seeking legal advice to ensure that their proposed use or disclosure of this information is for a purpose consistent with the purposes for which they received the information.

Australian Government
Department of Education

Your Ref
Our Ref LEX 50311

Secretary
Mr Tony Cook PSM

Mr Reece Kershaw
Commissioner
Australian Federal Police
GPO Box 401
CANBERRA CITY ACT 2601

Dear Mr Kershaw

Disclosure of protected information for the purposes of the Fraud Fusion Taskforce

Through ongoing correspondence with the Department of Education's (department) s22 , the Australian Federal Police (AFP) have requested the disclosure of protected information for the purposes of the AFP, including as they relate to the Fraud Fusion Taskforce.

I have authorised the disclosure of protected information to you as the Commissioner of the AFP for the purposes of the AFP (**Attachment A**).

This information remains protected information in the AFP's hands and may only be used for the purposes for which it was disclosed. To help the AFP's officers understand their obligations, I enclose a summary of legal advice given by the Australian Government Solicitor (**Attachment B**). Going forward, it will be the AFP's responsibility to safeguard the information and ensure it is only used, recorded and disclosed for the purposes of the AFP.

If you require any further assistance in this matter, please contact s22
.

Yours sincerely

[insert signature]

Tony Cook

[insert date]

OFFICIAL: Sensitive
Legal Privilege

A New Tax System (Family Assistance) (Administration) (Release of Protected Information) (AFP) Authorisation 2024

I, TONY COOK, Secretary of the Department of Education, acting under subparagraph 168(1)(b)(i) of the *A New Tax System (Family Assistance) (Administration) Act 1999*, authorise the disclosure of the protected information mentioned in Schedule 1 to the head of the Australian Federal Police (AFP) for the purposes of that authority.

Dated [Day Month Year]

[Insert signature]

---

1. Context

(1) The Department of Education (department) and the AFP are members of the Fraud Fusion Taskforce (FFT).

(2) The FFT is a partnership between the NDIA, Services Australia and 15 other government agencies (including the department and the AFP), which aims to detect, disrupt and prevent fraud and Serious and Organised Crime (SOC) with an objective to improve payment integrity across government programs.

(3) The department is providing information to the AFP that is relevant to the AFP's role as part of the operational arm of the wider FFT, supporting the Intelligence and Operations Committee Operational Working Group (IOC OWG). Specifically, the AFP will use their data to s37(2)(b) s47E(d) , complimenting ACIC data matching projects.

(4) The AFP will also be able to use that information for any purpose of the AFP, including but not limited to the purpose described in subsection (3).

2. Interpretation

(1) In this instrument, terms used have the same meaning that they have in the *A New Tax System (Family Assistance) (Administration) Act 1999*.

(2) In this instrument, unless the contrary intention appears:

Member agency or body of the Fraud Fusion Taskforce means any of the following:

(a) Department of Education (DE)
(b) National Disability Insurance Agency (NDIA)
(c) Services Australia
(d) Australian Criminal Intelligence Commission (ACIC)
(e) NDIS Quality and Safeguards Commission (NQSC)
(f) Attorney-General's Department (AGD)
(g) Australian Federal Police (AFP)
(h) Australian Tax Office (ATO)
(i) Commonwealth Director of Public Prosecutions (CDPP)
(j) Australian Securities & Investments Commission (ASIC)
(k) Australian Transaction Reports and Analysis Centre (AUSTRAC)
(l) Department of Health and Aged Care (DoHA)
(m) Department of Veterans' Affairs (DVA)
(n) Department of Employment and Workplace Relations (DEWR)
(o) Department of Social Services (DSS)
(p) Australian Skills Quality Authority (ASQA)
(q) Australian Charities and Not-for-Profits Commission (ACNC)
(r) Any other agency or body which joins the Fraud Fusion Taskforce subsequent to the making of this authorisation.

s37(2)(b) s47E(d)

3. Purpose of initial disclosure

(1) I am satisfied that the initial disclosure to the AFP described in subsection 1(3) is for the purposes of the AFP. Those purposes are described in the Australian Federal Police Act 1979 (AFP Act). In particular, the information supports the purpose described in section 8 of the AFP Act which includes "the provision of police services in relation to laws of the Commonwealth; the safeguarding of Commonwealth interests…", "the provision of police services and police support services for the purposes of assisting, or cooperating with, an Australian or foreign law enforcement agency…" and "anything incidental or conducive to the performance of the foregoing functions" listed throughout section 8.

(2) Subsection (1) does not, by implication, limit the purposes for which information is disclosed under this instrument, being "for the purposes of that authority".

Schedule 1— Information able to be disclosed

The following information may be disclosed:

Information about providers

s37(2)(b) s47E(d)

Legal Advice

The following summary of legal advice given by the Australian Government Solicitor is provided pursuant to the *Legal Services Directions 2017*. Legal privilege is not waived.

s42(1)

The agency receiving protected information is responsible for seeking legal advice to ensure that their proposed use or disclosure of this information is for a purpose consistent with the purposes for which they received the information.

Document 7

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

……
ACIC
…… day 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

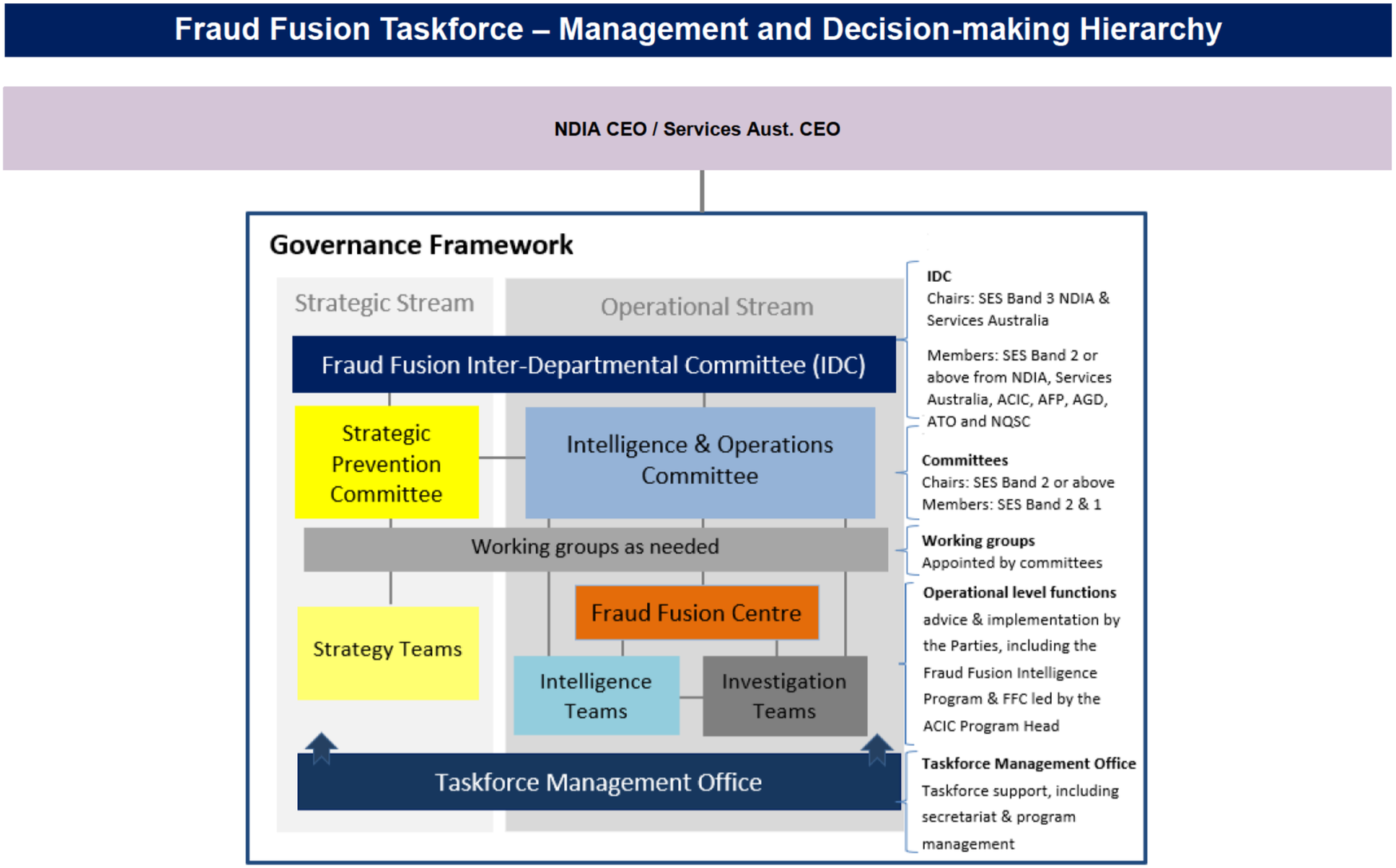
ABN 36 342 015 855

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 Government
Department of Education

[Name of Data Recipient]
[Position]
[Agency Name]
[Address]

Dear [Name of Data Recipient]

NOTICE TO RECIPIENT OF DEPARTMENT OF EDUCATION INFORMATION
Section 168 of the A New Tax System (Family Assistance) (Administration) Act 1999

I am writing to you about the disclosure of certain protected information by the Department of Education (the department) to the [Agency Name] under section 168 of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Administration Act).

The Secretary, or their delegate, may authorise the disclosure of protected information under paragraph 168(1)(a) of the Administration Act by issuing a Public Interest Certificate (PIC). Before giving the PIC, the delegate must be satisfied that it is necessary in the public interest to do so in a particular case or class of cases consistent with the Family Assistance (Public Interest Certificate Guidelines) (Education) Determination 2018 (PIC Guidelines).

The relevant delegate issued PIC [insert relevant PIC number] on [date]. This PIC, made under section 9 of the PIC Guidelines, authorises the disclosure of protected information to [Agency Name] and other partner agencies comprising the Commonwealth Fraud Fusion Taskforce (FFT) for enforcement related activities undertaken as part of the FFT.

The following sections outline the purpose of this disclosure, as well as any limitations on how [Agency Name] may use, record or disclose the information.

Background

The department has portfolio responsibility for supporting the Australian Government's commitment to affordable early childhood education and care (ECEC) and directly delivers several core operational functions to support Child Care Subsidy (CCS) financial integrity, including Provider Approvals, Integrity Capability and Engagement, Compliance Operations, Fraud Investigations and Tactical Operations, Provider Audits, CCS Helpdesk and Strategic Communication.

The department has extensive CCS data and intelligence holdings to contribute to the key objectives of the FFT. s37(2)(b) s47E(d)

Purpose for the disclosure of Department of Education information

The department will support the FFT to achieve its objective by sharing data and information relating to s37(2)(b) s47E(d)

[ACIC/AFP]

[NOTE: only use where disclosure is not authorised under the secretary disclosure notice]

At a high level, disclosure of this information enables [Agency Name] to perform enforcement-related activities, whether undertaken as part of the Fraud Fusion Taskforce or not.

[OTHER PARTNER AGENCIES]

At a high level, disclosure of this information enables [Agency Name] to perform enforcement-related activities, undertaken as part of the Fraud Fusion Taskforce.

A delegate has certified that, in accordance with:

- paragraph 168(1)(a) of the Administration Act; and
- the purpose for disclosure provided for in section 9 of the PIC Guidelines,

it is necessary in the public interest to disclose this information to [Agency Name] as a member agency of the FFT.

Description of the relevant information that will be shared by Department of Education

Attached to this notice are [NUMBER] data sets containing protected information under the Administration Act.

Data set 1 – [description of dataset]

Data set 2 – [description of dataset]

Permitted use and disclosure of the relevant information

After the relevant information has been disclosed by the department, [Agency Name] may only use it for the purpose described in section [insert number] of PIC CC [insert relevant PIC number] (see Attachment A of this notice).

[Agency Name] may not use or otherwise disclose the relevant information, for any other purpose, project or activity unless required or authorised by law. Written consent must be provided by the department prior to any further use, or disclosure by the receiving agency, and the department will consider whether the proposed use or disclosure is permitted under the FAL, including for the purposes of the PIC, or whether a new PIC or other legal arrangement is required.

Yours sincerely

_____

[Name]
[Position]
Intelligence Analytics, Financial Integrity Branch
Department of Education

[Date]

OFFICIAL: Sensitive
Personal Privacy

Australian Government
Department of Education

[Name of Data Recipient]
[Position]
[Agency Name]
[Address]

Dear [Name of Data Recipient]

NOTICE TO RECIPIENT OF DEPARTMENT OF EDUCATION INFORMATION
Section 168(1)(b)(i) of the A New Tax System (Family Assistance) (Administration) Act 1999

I am writing to you about the disclosure of certain protected information by the Department of Education (the department) to the [Australian Criminal Intelligence Commission (ACIC)/Australian Federal Police (AFP)] under section 168(1)(b)(i) of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Administration Act).

The Secretary of the department may disclose protected information under paragraph 168(1)(b)(i) of the Administration Act to the Secretary of a Commonwealth department or to the Agency Head of an authority of the Commonwealth for the purposes of that department/authority.

The following sections outline the purpose of this disclosure, as well as any limitations on how the [ACIC/AFP] may use, record or disclose the information.

Background

The department has portfolio responsibility for supporting the Australian Government's commitment to affordable early childhood education and care (ECEC) and directly delivers several core operational functions to support Child Care Subsidy (CCS) financial integrity, including Provider Approvals, Integrity Capability and Engagement, Compliance Operations, Fraud Investigations and Tactical Operations, Provider Audits, CCS Helpdesk and Strategic Communication.

The department has extensive CCS data and intelligence holdings to contribute to the key objectives of the FFT. s37(2)(b) s47E(d)

s

s37(2)(b) s47E(d)

Purpose for the disclosure of Department of Education information

The department will support the FFT to achieve its objective by sharing data and information relating to s37(2)(b) s47E(d)

[ACIC]

At a high level, disclosure of this information enables the ACIC to perform its functions under the *Australian Crime Commission Act 2002* (Cth) (ACC Act) including the collection, correlation, analysis and dissemination of criminal information and intelligence to member agencies of the FFT.

Specifically, the information will enable the FFT to s37(2)(b) s47E(d)

This matching process will feed into s37(2)(b) s47E(d) and fraud prevention at the strategic level.

[AFP]

At a high level, disclosure of this information enables the AFP to perform its functions under the Australian Federal Police Act 1979 (AFP Act). In particular, the information supports the purpose described in section 8(1)(b) of the AFP Act: "the provision of police services in relation to laws of the Commonwealth; the safeguarding of Commonwealth interests…".

Specifically, the information will enable the FFT to s37(2)(b) s47E(d)

. This matching process will feed into s37(2)(b) s47E(d) and fraud prevention at the strategic level.

AFP will use their data to s37(2)(b) s47E(d)

, complimenting ACIC data matching projects.

Description of the relevant information that will be shared by Department of Education

Attached to this notice are [NUMBER] data sets containing protected information under the Administration Act.

Data set 1 – [description of dataset]

Data set 2 – [description of dataset]

Permitted use and disclosure of the relevant information

[ACIC]

After the relevant information has been disclosed by the department, the ACIC may only use or disclose it for the purposes of the ACIC, as described in section 7A of the ACC Act, including as they relate to the FFT.

The ACIC may not use or otherwise disclose the relevant information for any other purpose, project or activity unless required or authorised by law. You must not use or disclose the information for such other purposes without the department's written consent. This will enable the department to consider and, if necessary, ensure there is legal authority for the use or disclosure.

[AFP]

After the relevant information has been disclosed by the department, the AFP may only use or disclose it for the purposes of the AFP, as described in section 8(1)(b) of the AFP Act, including as they relate to the FFT.

The AFP may not use or otherwise disclose the relevant information for any other purpose, project or activity unless required or authorised by law. You must not use or disclose the information for such other purposes without the department's written consent. This will enable the department to consider and, if necessary, ensure there is legal authority for the use or disclosure.

Yours sincerely

_____

[Name]
[Position]
Intelligence Analytics, Financial Integrity Branch
Department of Education

[Date]