



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence, a coordinated government approach to detection and treatment of serious and organised crime and systemic fraud and well-informed cross-program actions to help prevent fraud. This will draw on the capabilities and powers of the agencies that are parties to the Memorandum of Understanding for the Fraud Fusion Taskforce (MOU). This project is specific to the treatment and management of information sharing between Department of Employment and Workplace Relations (DEWR) and the Taskforce's Fraud Fusion Centre; established, operated and led by the Australian Criminal Intelligence Commission (ACIC).
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Enterprise Risk, Assurance and Investigations Branch, Legal and Assurance Division, DEWR Compliance Intelligence, Skills Program Compliance Branch, Skills and Training Group, DEWR

FEG Program Management Office, Entitlements Safeguards Division, Workplace Relations Group, DEWR
Assurance Insights, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR
Risk Management Insurance Incidents, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR
External Stakeholder/s:
ACIC-led Fraud Fusion Centre (FFC)

Section 1: Personal information

Type of information	Collect	Use	Disclose	Store	Destroy ²	De-identify
Names	☐	☒	☒	☒	☐	☐
Signatures	☐	☒	☒	☒	☐	☐
Addresses	☐	☒	☒	☒	☐	☐
Email addresses	☐	☒	☒	☒	☐	☐
Telephone numbers	☐	☒	☒	☒	☐	☐
Dates of birth	☐	☒	☒	☒	☐	☐
Sex or gender	☐	☒	☒	☒	☐	☐
Opinions or feedback	☐	☒	☒	☒	☐	☐
Commentary	☐	☒	☒	☒	☐	☐
CRNs or JSIDs	☐	☒	☒	☒	☐	☐
USIs or CHESSNs	☐	☒	☒	☒	☐	☐
Tax file numbers	☐	☒	☐	☒	☐	☐
Financial information	☐	☒	☒	☒	☐	☐
Bank account details	☐	☒	☒	☒	☐	☐

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Commented s 22(1): Paragraph B.146 of the Australian Privacy Principle Guidelines issued by the Office of the Australian Information Commissioner provides 'Generally, an APP entity uses personal information when it handles and manages that information within the entity's effective control.'

Commented s 22(1): Paragraph B.67 of the Australian Privacy Principle Guidelines issued by the Office of the Australian Information Commissioner provides 'An APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.'

Identity documents	☐	☒	☒	☒	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
The Fraud Team is very unlikely to use or store other types of personal or sensitive information unless it is relevant to a criminal investigation. For example, personal and sensitive information such as relationship status and involvement in family and domestic violence.						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative:						
You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.						
The ACIC-led Fraud Fusion Centre will initiate and facilitate information sharing, issuing Requests for Information (RFIs) via electronic mail (email) to the DEWR Fraud Fusion Taskforce mailbox. The RFIs may contain personal information of individuals and/or entities which have been approved for release under section 59AA of the <i>Australian Crime Commission Act 2002</i> (Cth), and which is permitted for internal dissemination under the Australian Privacy Principle (APP) 6 for cross-referencing purposes.						
The nature of information collected will vary depending on each RFI. ESSWeb, ADMS, iBase, ESS Tip-off system, FEG systems will be used as sources to respond to probity checks specific to the RFI.						
Information collected and prepared for disclosure to the Taskforce will occur in accordance with appropriate legislation and clearance from the Information Legal Team. Each request will be considered carefully and released in line with relevant legislation and personal information management requirements. It is anticipated a Public Information Certificate (PIC) will be considered for each release of information.						

Commented s 22(1) Please ensure you include the following details:

- Where the personal information will be stored
- Who will have access to the personal information, including any access by cloud or software providers
- If personal information will be disclosed to a third party, how the personal information will be shared (eg by email or Secure File Transfer Protocol)
- If personal information will be stored on the cloud, whether the servers are located in Australia or overseas

Release of information will most typically be in the form of an email to the FFC mailbox, classification 'Official: Sensitive', or by File Transfer, and be accessed by ACIC-led Fraud Fusion Taskforce Officers.

Information shared will be stored in XXXXXX (eg O Drive, Content Manager). Access to the DEWR Fraud Fusion Taskforce mailbox, O Drive and Content Manager will be restricted to persons authorised by XXXXX and will require to hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) and procedures in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Where the personal information will be stored:

Who will have access to the personal information, including any access by cloud or software providers:

If personal information will be disclosed to a third party, how the personal information will be shared (eg by email or Secure File Transfer Protocol):

If personal information will be stored on the cloud, whether the servers are located in Australia or overseas:

How many individuals' personal or sensitive information will be handled in the project or initiative?

TBC

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes

- | | |
|-------------------------------------|---|
| ☐ | The <u>nature or type</u> of the personal information being handled is new or different. |
| ☒ | The <u>scope</u> of the personal information being handled is new or different. |
| ☒ | The personal information is being handled in a new or different <u>context</u> . |
| ☒ | The <u>purpose</u> for which the personal information is being handled is new or different. |
| ☐ | The <u>risk</u> of handling the personal information is new or different. |

If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).

Commented s 22(1) There is a new or changed way of handling personal information if any of the following apply:

- The handling relates to a completely new function or activity
- The department will be collecting more personal information than it used to or initiating a new collection
- The department will be using or disclosing the personal information for a different purpose than previously, including movement from paper based to electronic
- The department will be disclosing personal information to a third party that has not previously been disclosed
- A change is being made to how the personal information will be stored or disclosed
- A change is being made to who will have access to the personal information

If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).

You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.

Commented s 22(1) There needs to be more in common than just the means of handling (eg by email) for this to apply.

In addition, a privacy threshold assessment must have already been completed for the existing practice the handling is being compared to.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?

Potentially

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:

- ☒ Handling large amounts of personal information.
- ☒ Handling sensitive information³.
- ☒ Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
- ☐ Handling the personal information of individuals who are vulnerable.⁴
- ☐ Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
- ☒ Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
- ☒ Using or disclosing personal information for profiling or behavioural predictions.
- ☐ Using personal information for automated decision-making.
- ☐ Collecting personal information through systematic monitoring or tracking of individuals.
- ☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
- ☒ Using information for data matching or linking unconnected personal information.
- ☒ Developing legislation to modify the operation of the *Privacy Act 1988* or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
- ☒ Handling personal information for activities of a long term or permanent duration.

Commented s 22(1) Whether a project or initiative is likely to have a significant impact on privacy depends on a range of factors.

The more of the factors below that apply the more likely the project or initiative is to have a significant impact on privacy. This includes if a security assessment has given the project or initiative a medium or high risk rating it should be considered as being likely to have a significant impact on privacy.

Commented s 22(1) This factor encompasses consideration of both the number of individuals whose personal information is being handled, the volume of personal information about those individuals, and the number of people internally and externally who have access to that personal information.

Commented s 22(1); This factor requires consideration of the potential consequences for the individual in the handling, and any potential mishandling, of their personal information. For example, if bank account details are involved there is the potential for financial loss from unauthorised access.

Commented s 22(1) This factor will apply if the project or initiative will be running for more than 3 months.

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
Information related to criminal investigations into individuals, if subject to unauthorised access and release, could significantly damage reputation and wellbeing.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	Choose an item.
I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.	

Approved by: **s 22(1)** Assistant Secretary and Chief Internal Auditor

Date: Click or tap to enter a date.

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and <u>intelligence</u>. <u>The Taskforce along with the with the Taskforce's Fraud Fusion Centre (FFC) is operated, co-ordinated and led by the Australian Criminal Intelligence Commission (ACIC).</u> <u>The purposes of ACIC is 'to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence' (as set out under section 7A of the Australian Crime Commission Act 2002).</u> <u>a coordinated government approach to detection and treatment of serious and organised crime and systemic fraud and well-informed cross-program actions to help prevent fraud. This will draw on the capabilities and powers of the agencies that are parties to the Memorandum of Understanding for the Fraud Fusion Taskforce (MOU).</u> This project is <u>seeking a streamlined approach specific to the treatment and management of information sharing between the Department of Employment and Workplace Relations (DEWR) and the Taskforce's Fraud Fusion Centre (FFC) as noted on the Fraud Fusion Taskforce Memorandum of Understanding (MOU).</u>
--	--

Commented s 22(1) Does the ACIC also lead the taskforce?
Or is that the NDIA?

established, operated and led by the Australian Criminal Intelligence Commission (ACIC). Mult
The MOU notes:

1. the Taskforce seeks to understand, prevent, respond to and disrupt fraud and criminal activity against various government programs, including serious organised crime (SOC), by sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs (see subclause 5-4(a));

2. the Taskforce seeks to enhance government co-ordination to prevent, detect, and respond to fraud and related criminal activity within and against government programs by collecting, correlating, analysing and disseminating information and intelligence to develop appropriate responses to criminal activity, and fraud, including SOC (see subclause 5-4(c)(iii));

3. the Fraud Fusion Intelligence Program will be established and independently managed by ACIC and oversee the activities of the FFC, including its administration, intelligence development and data sharing (see subclause 7-7(d))

4. the Fraud Fusion intelligence program will serve as the Taskforce's centrepiece for intelligence collection, correlation, analysis and dissemination (see subclause 7-7(e)); and

5. the FFC will be established, operated and led by ACIC (see subclause 7-8(b))

DEWR may release information in one of two ways:

- a request for information initiated by the FFC, or
- DEWR believes information held is within the remit of the Taskforce MOU, i-agency capability and

Commented ^{s 22(1)} Does the ACIC also lead the taskforce? Or is that the NDIA?

Formatted: Space After: Auto, Line spacing: 1.5 lines, Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0.63 cm

Commented ^{s 22(1)} : Can you please check these?

Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Enterprise Risk, Assurance and Investigations Branch, Legal and Assurance Division, DEWR Compliance Intelligence, Skills Program Compliance Branch, Skills and Training Group, DEWR FEG Program Management Office, Entitlements Safeguards Division, Workplace Relations Group, DEWR Assurance Insights, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR Risk Management Insurance Incidents, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR External Stakeholder/s: ACIC led Fraud Fusion Centre (FFC)

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.		Yes				
Type of information	Collect	Use	Disclose	Store	Destroy ²	De-identify
Names	☐	☒	☒	☒	☐	☐
Signatures	☐	☒	☒	☒	☐	☐
Addresses	☐	☒	☒	☒	☐	☐
Email addresses	☐	☒	☒	☒	☐	☐
Telephone numbers	☐	☒	☒	☒	☐	☐

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Commented s 22(1) Paragraph 8.146 of the Australian Privacy Principle Guidelines issued by the Office of the Australian Information Commissioner provides 'Generally, an APP entity uses personal information when it handles and manages that information within the entity's effective control.'

Commented s 22(1) Why have we ticked Use? Are we ticking this because we are going to use the info ourselves?

Commented s 22(1) Paragraph 8.67 of the Australian Privacy Principle Guidelines issued by the Office of the Australian Information Commissioner provides 'An APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.'

Dates of birth	☐	☒	☒	☒	☐	☐
Sex or gender	☐	☒	☒	☒	☐	☐
Opinions or feedback	☐	☒	☒	☒	☐	☐
Commentary	☐	☒	☒	☒	☐	☐
CRNs or JSIDs	☐	☒	☒	☒	☐	☐
USIs or CHESSNs	☐	☒	☒	☒	☐	☐
Tax file numbers	☐	☒	☐	☒	☐	☐
Financial information	☐	☒	☒	☒	☐	☐
Bank account details	☐	☒	☒	☒	☐	☐
Identity documents	☐	☒	☒	☒	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
The Fraud Team is very unlikely to use or store other types of personal or sensitive information unless it is relevant to a criminal investigation. For example, personal and sensitive information such as relationship status and involvement in family and domestic violence. N/A						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative:						
You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.						
<u>Request for Information (RFI)</u>						
The <u>FFC ACIC led Fraud Fusion Centre</u> will initiate and facilitate information sharing, issuing <u>an Requests for Information (RFI/s)</u> via <u>electronic mail (email)</u> to the DEWR Fraud Fusion Taskforce mailbox. The RFI/s may contain personal information of individuals and/or entities which have been approved for release under section 59AA of the <i>Australian Crime Commission Act 2002</i> (Cth),						

Commented s 22(1) don't think this is relevant. We are talking about sharing the information, not what happens during an investigation.

Commented s 22(1) Please ensure you include the following details:

- Where the personal information will be stored
- Who will have access to the personal information, including any access by cloud or software providers
- If personal information will be disclosed to a third party, how the personal information will be shared (eg by email or Secure File Transfer Protocol)
- If personal information will be stored on the cloud, whether the servers are located in Australia or overseas

Formatted: Underline

and which is permitted for internal dissemination under the Australian Privacy Principle (APP) 6 for cross-referencing purposes.

Release of Information

Formatted: Underline

The Fraud Team through an intelligence lead process may initiate a release of information, if it believes the information will help facilitate a whole of Government approach to the detection, prevention and treatment of serious or systemic fraud.

Collected

Formatted: Underline

The nature of information collected will vary depending on each RFI or release, we believe the information collected will fall within these categories:

- (a) material that is both personal and protected information;
- (b) material that is personal but not protected information; and
- (c) material that is neither personal nor protected information (where the information has not been obtained under any law and relates to a business or person).

*The information will be sourced from either various department managed systems e.g., ESSWeb, ADMS, TYIMS, FEGiBase, ESS Tip-off system and, iBase. FEG systems will be used as sources to respond to probity checks specific to the RFI.

Additional information will be sourced through paid third parties e.g., Equifax or open source such as ABN lookup or Google.

Stored

Formatted: Underline

Information will be stored in the O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox and/or by the departments web based secure File Transfer system. Access to the Fraud Fusion Taskforce mailbox, O Drive, Content Manager and File Transfer will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

Commented s 22(1) We may have to choose which one.

The internal DEWR server is compliant with the Information Management Policy, and adheres to the Information Security Handbook and procedures in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Disclosure

Information collected and prepared for disclosure to the Taskforce will occur in accordance with appropriate legislation and clearance from the Information Legal Team (ILT). Each request will be considered carefully and released in line with relevant legislation and personal information

management requirements. It is anticipated a Public Information Certificate (PIC) will be considered for each release of information.

Commented s 22(1) Is this required if we do a PIC

Release of information will most typically be in the form of an email to the FFC mailbox, classification 'Official: Sensitive', or by File Transfer, and be accessed by ~~ACIC led Fraud Fusion~~ Taskforce Officers.

~~Information shared will be stored in XXXXXX (eg O Drive, Content Manager). Access to the DEWR Fraud Fusion Taskforce mailbox, O Drive and Content Manager will be restricted to persons authorised by XXXXX and will require to hold a Negative Vetting Level 1 clearance.~~

~~The internal DEWR server is compliant with the Information Management Policy, and adheres to the Information Security Handbook and procedures in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.~~

~~Where the personal information will be stored:~~

~~Who will have access to the personal information, including any access by cloud or software providers:~~

~~If personal information will be disclosed to a third party, how the personal information will be shared (eg by email or Secure File Transfer Protocol):~~

~~If personal information will be stored on the cloud, whether the servers are located in Australia or overseas:~~

How many individuals' personal or sensitive information will be handled in the project or initiative?

TBC

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?	
If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.	Yes
☐ The <u>nature</u> or <u>type</u> of the personal information being handled is new or different.	
☒ The <u>scope</u> of the personal information being handled is new or different.	
☒ The personal information is being handled in a new or different <u>context</u> .	
☒ The <u>purpose</u> for which the personal information is being handled is new or different.	

Commented s 22(1) There is a new or changed way of handling personal information if any of the following apply:

- The handling relates to a completely new function or activity
- The department will be collecting more personal information than it used to or initiating a new collection
- The department will be using or disclosing the personal information for a different purpose than previously, including movement from paper based to electronic
- The department will be disclosing personal information to a third party that has not previously been disclosed
- A change is being made to how the personal information will be stored or disclosed
- A change is being made to who will have access to the personal information

 The <u>risk</u> of handling the personal information is new or different.
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).
You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.

Commented s 22(1): There needs to be more in common than just the means of handling (eg by email) for this to apply.

In addition, a privacy threshold assessment must have already been completed for the existing practice the handling is being compared to.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?	Potentially
To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	
☒ Handling large amounts of personal information.	
☒ Handling sensitive information ³ .	
 Handling personal information in a way that is likely to raise public concern or unlikely to have community support.	
☐ Handling the personal information of individuals who are vulnerable. ⁴	
☐ Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.	
☒ Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.	
☒ Using or disclosing personal information for profiling or behavioural predictions.	
☐ Using personal information for automated decision-making.	
☐ Collecting personal information through systematic monitoring or tracking of individuals.	
☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.	
☒ Using information for data matching or linking unconnected personal information.	

Commented s 22(1) Whether a project or initiative is likely to have a significant impact on privacy depends on a range of factors.

The more of the factors below that apply the more likely the project or initiative is to have a significant impact on privacy. This includes if a security assessment has given the project or initiative a medium or high risk rating it should be considered as being likely to have a significant impact on privacy.

Commented s 22(1): This factor encompasses consideration of both the number of individuals whose personal information is being handled, the volume of personal information about those individuals, and the number of people internally and externally who have access to that personal information.

Commented s 22(1) This factor requires consideration of the potential consequences for the individual in the handling, and any potential mishandling, of their personal information. For example, if bank account details are involved there is the potential for financial loss from unauthorised access.

Commented s 22(1) Not sure about this one, I would say we are using info we already have, but are you thinking more RPI's from ACIC that has info we don't store already.

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

☒	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
Information related to criminal investigations into individuals, if subject to unauthorised access and release, could significantly damage reputation and wellbeing.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Commented S 22(1) This factor will apply if the project or initiative will be running for more than 3 months.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	Choose an item.
I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.	

Approved by: **S 22(1)** Assistant Secretary and Chief Internal Auditor

Date: Click or tap to enter a date.

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence. The Taskforce along with the Taskforce's Fraud Fusion Centre (FFC) is operated, co-ordinated and led by the Australian Criminal Intelligence Commission (ACIC). The purpose of ACIC is 'to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence' (as set out under section 7A of the <i>Australian Crime Commission Act 2002</i>). This project is seeking a streamlined approach to the treatment and management of information sharing between the Department of Employment and Workplace Relations (DEWR) and the Taskforce's Fraud Fusion Centre (FFC) as noted in the Fraud Fusion Taskforce Memorandum of Understanding (MOU). The MOU notes: 1. The Taskforce seeks to understand, prevent, respond to and disrupt and criminal activity against various government programs, including serious organised crime (SOC), by sharing data and information in order to improve integrity through analysing data to
--	--

	identify potential fraud and associated behaviours affecting government payments and programs (see subclause 5-4(a)); 2. The Taskforce seeks to enhance government co-ordination to prevent, detect, and respond to fraud and related criminal activity within and against government programs by collecting, correlating, analysing and disseminating information and intelligence to develop appropriate responses to criminal activity, and fraud, including SOC (see subclause 5-4(c)(ii)); 3. The Fraud Fusion Intelligence Program will be established and independently managed by ACIC and oversee the activities of the FFC, including its administration, intelligence development and data sharing (see subclause 7-7(d)); 4. The Fraud Fusion Intelligence Program will serve as the Taskforce's centrepiece for intelligence collection, correlation, analysis and dissemination (see subclause 7-7(e); and 5. The FFC will be established, operated and led by the ACIC 9see subclause 7-8(b)). DEWR may release information in one of two ways: (a) in response to a request for information initiated by the FFC, or (b) DEWR believes information held in within the remit of the Taskforce MOU.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Enterprise Risk, Assurance and Investigations Branch, Legal and Assurance Division, DEWR Compliance Intelligence, Skills Program Compliance Branch, Skills and Training Group, DEWR

	FEG Program Management Office, Entitlements Safeguards Division, Workplace Relations Group, DEWR
	Assurance Insights, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR
	Risk Management Insurance Incidents, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR
	External Stakeholder/s:
	ACIC

Section 1: Personal information

Type of information	Collect	Use	Disclose	Store	Destroy ²	De-identify
Names	☐	☒	☒	☒	☐	☐
Signatures	☐	☒	☒	☒	☐	☐
Addresses	☐	☒	☒	☒	☐	☐
Email addresses	☐	☒	☒	☒	☐	☐
Telephone numbers	☐	☒	☒	☒	☐	☐
Dates of birth	☐	☒	☒	☒	☐	☐
Sex or gender	☐	☒	☒	☒	☐	☐
Opinions or feedback	☐	☒	☒	☒	☐	☐
Commentary	☐	☒	☒	☒	☐	☐
CRNs or JSIDs	☐	☒	☒	☒	☐	☐
USIs or CHESSNs	☐	☒	☒	☒	☐	☐
Tax file numbers	☐	☒	☐	☒	☐	☐
Financial information	☐	☒	☒	☒	☐	☐
Bank account details	☐	☒	☒	☒	☐	☐

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Commented s 22(1) Paragraph B.146 of the Australian Privacy Principle Guidelines issued by the Office of the Australian Information Commissioner provides 'Generally, an APP entity uses personal information when it handles and manages that information within the entity's effective control.'

Commented s 22(1) Why have we ticked Use? Are we ticking this because we are going to use the info ourselves?

Commented s 22(1) Yes

Commented s 22(1); Paragraph B.67 of the Australian Privacy Principle Guidelines issued by the Office of the Australian Information Commissioner provides 'An APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.'

Identity documents	☐	☒	☒	☒	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/A						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative:						
You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.						
<u>Request for Information (RFI)</u>						
The FFC will initiate and facilitate information sharing, issuing an RFI/s via the DEWR Fraud Fusion Taskforce mailbox. The RFI/s may contain personal information of individuals and/or entities which have been approved for release under section 59AA of the <i>Australian Crime Commission Act 2002</i> (Cth), and which is permitted for internal dissemination under the Australian Privacy Principle (APP) 6 for cross-referencing purposes.						
<u>Release of Information</u>						
The Fraud Team through an intelligence lead process may initiate a release of information, if it believes the information will help facilitate a whole of Government approach to the detection, prevention and treatment of serious or systemic fraud.						
<u>Collected</u>						

Commented | s 22(1) Amended

Commented s 22(1); Please ensure you include the following details:

- Where the personal information will be stored
- Who will have access to the personal information, including any access by cloud or software providers
- If personal information will be disclosed to a third party, how the personal information will be shared (eg by email or Secure File Transfer Protocol)
- If personal information will be stored on the cloud, whether the servers are located in Australia or overseas

The nature of information collected will vary depending on each RFI or release; we believe the information collected will fall within these categories:

- (a) material that is both personal and protected information;
- (b) material that is personal but not protected information; and
- (c) material that is neither personal nor protected information (where the information has not been obtained under any law and relates to a business or person).

The information may be sourced from various department managed systems e.g., ESS, ADMS, TYIMS, FEG, ESS Tip-off and iBase.

Additional information may be sourced through paid third parties e.g., Equifax or open source such as ABN lookup or Google.

Stored

Information will be stored in the O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox and/or by the departments web based secure File Transfer system. Access to the Fraud Fusion Taskforce mailbox, O Drive, Content Manager and File Transfer will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the Information Management Policy, and adheres to the Information Security Handbook and procedures in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Disclosure

Information collected and prepared for disclosure to the Taskforce will occur in accordance with appropriate legislation and clearance from the Information Legal Team (ILT). Each request will be considered carefully and released in line with relevant legislation and personal information management requirements. It is anticipated a Public Information Certificate (PIC) may be considered for each release of information.

Release of information will most typically be in the form of an email to the FFC mailbox, classification 'Official: Sensitive', or by File Transfer, and be accessed by Taskforce Officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?

TBC

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?	Yes
---	-----

Commented s 22(1) We may have to choose which one.

Commented s 22(1) : Something to discuss with
s11C(1)(a) s11C(1)(a)

Commented s 22(1) : Is this required if we do a PIC

Commented [S 22(1)] Have inserted, 'may'

Commented S 22(1) There is a new or changed way of handling personal information if any of the following apply:

- The handling relates to a completely new function or activity
- The department will be collecting more personal information than it used to or initiating a new collection
- The department will be using or disclosing the personal information for a different purpose than previously, including movement from paper based to electronic
- The department will be disclosing personal information to a third party that has not previously been disclosed
- A change is being made to how the personal information will be stored or disclosed
- A change is being made to who will have access to the personal information

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.	
☐	The <u>nature or type</u> of the personal information being handled is new or different.
☒	The <u>scope</u> of the personal information being handled is new or different.
☒	The personal information is being handled in a new or different <u>context</u> .
☒	The <u>purpose</u> for which the personal information is being handled is new or different.
☒	The <u>risk</u> of handling the personal information is new or different.
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).	
You should provide the name of the same or similar project or initiative <u>where the practice(s) have been assessed previously</u> and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	

Commented s 22(1) There needs to be more in common than just the means of handling (eg by email) for this to apply.

In addition, a privacy threshold assessment must have already been completed for the existing practice the handling is being compared to.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?	Potentially
To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	
☒	Handling large amounts of personal information.
☒	Handling sensitive information ³ .
☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
☐	Handling the personal information of individuals who are vulnerable. ⁴
☐	Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.

Commented s 22(1) Whether a project or initiative is likely to have a significant impact on privacy depends on a range of factors.

The more of the factors below that apply the more likely the project or initiative is to have a significant impact on privacy. This includes if a security assessment has given the project or initiative a medium or high risk rating it should be considered as being likely to have a significant impact on privacy.

Commented s 22(1) : This factor encompasses consideration of both the number of individuals whose personal information is being handled, the volume of personal information about those individuals, and the number of people internally and externally who have access to that personal information.

Commented s 22(1) This factor requires consideration of the potential consequences for the individual in the handling, and any potential mishandling, of their personal information. For example, if bank account details are involved there is the potential for financial loss from unauthorised access.

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

☒	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☒	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.
☒	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☒	Using information for data matching or linking unconnected personal information.
☒	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Commented s 22(1) ot sure about this one, I would say we are using info we already have, but are you thinking more RPI's from ACIC that has info we don't store already.

Commented s 22(1): Yes, although we have not initiated the collecting of information we are collecting information as a result of the RFI. Happy to discuss.

Commented s 22(1) This factor will apply if the project or initiative will be running for more that 3 months.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	Choose an item.
I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.	

Approved by: S 22(1) Assistant Secretary and Chief Internal Auditor

Date: Click or tap to enter a date.

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).

Document 4 (page 22-28) deleted under section 42(1) of the *Freedom of Information Act 1982* (Cth).

Document 5 (page 29-36) deleted under section 42(1) of the *Freedom of Information Act 1982* (Cth).



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence. The Taskforce along with the Taskforce's Fraud Fusion Centre (FFC) is operated, co-ordinated and led by the Australian Criminal Intelligence Commission (ACIC). The purpose of ACIC is 'to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence' (as set out under section 7A of the <i>Australian Crime Commission Act 2002</i>). This project is seeking a streamlined approach to the treatment and management of information sharing between the department and the FFC as noted in the Fraud Fusion Taskforce Memorandum of Understanding (MOU). s 42(1) (a) in response to a request for information initiated by the FFC, or (b) proactively – when information held by the department is considered to be within the remit of the Taskforce MOU.
--	--

s 42(1)

	The department does not have control or oversight as to the type of information collected by the ACIC and shared to Taskforce partner agencies for data matching. The department will manage incoming data releases from the FFC in line with the Taskforce Data Governance Framework. The MOU notes: 1. The Taskforce seeks to understand, prevent, respond to and disrupt criminal activity against various government programs, including serious organised crime (SOC), by sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs. 2. The Taskforce seeks to enhance government co-ordination to prevent, detect, and respond to fraud and related criminal activity within and against government programs by collecting, correlating, analysing, and disseminating information and intelligence to develop appropriate responses to criminal activity, and fraud, including SOC. 3. The Fraud Fusion Intelligence Program will be established and independently managed by ACIC and oversee the activities of the FFC, including its administration, intelligence collection, development, and data sharing.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Compliance Intelligence Team FEG Program Management Office Assurance Insights Team Risk Management Insurance Incidents Team External Stakeholder/s: ACIC

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information ¹ ?			Yes			
- If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						
Type of information	Collect	Disclose	Store	Destroy ²	De-identify	
Names	☐	☒	☒	☒	☐	☐
Signatures	☐	☒	☒	☒	☐	☐
Addresses	☐	☒	☒	☒	☐	☐
Email addresses	☐	☒	☒	☒	☐	☐
Telephone numbers	☐	☒	☒	☒	☐	☐
Dates of birth	☐	☒	☒	☒	☐	☐
Sex or gender	☐	☒	☒	☒	☐	☐
Opinions or feedback	☐	☒	☒	☒	☐	☐
Commentary	☐	☒	☒	☒	☐	☐
CRNs or JSIDs	☐	☒	☒	☒	☐	☐
USIs or CHESSNs	☐	☒	☒	☒	☐	☐
Tax file numbers	☐	☒	☐	☒	☐	☐
Financial information	☐	☒	☒	☒	☐	☐
Bank account details	☐	☒	☒	☒	☐	☐
Identity documents	☐	☒	☒	☒	☐	☐
	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☒	☒	☒	☐	☐

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

s 42(1)

Commented s 22(1) There is a technical issue 'ticking' boxes for 'Collect' column.

s 42(1)

s 42(1)

Commented s 22(1) This cannot be confirmed. The collection of, or disclosing of 'racial or ethnic origin' information is dependent on the scope of the investigation and significance this information may have on the investigation or operation. At best, the probability (or risk factor) of this information being needed is low, but cannot be wholly excluded.

Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/A						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?						
You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, how information will be stored in the cloud and who information will be disclosed to and why.						

s 42(1)

s 42(1)

The Request For Information (RFI)s received from the FCC may contain personal information of individuals and/or entities that have been approved for release under section 59AA of the Australian Crime Commission Act 2002 (Cth) with the intention to generate intelligence and insights from partner agencies.

Information received from the FCC will include tactical and strategic intelligence products addressing criminal and risk indicate activity insights. These will be used to inform administrative data sharing and individual agency activity.

It is the role of the ACIC to determine the type of information, including personal information, to be shared with partner agencies.

s 42(1)

s 42(1)

The department will collate personal information it holds in preparation for disclosure if requested by the FCC under an RFI or it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

The department will manage incoming data requests by following practicable actions:

- (a) consult with the Taskforce on the scope of a RFI; its operational significance and required actions (in 28 days??)
- (b) inform the relevant delegate of the RFI
- (c) work with departmental business areas (primarily compliance areas) to identify department's information and data holdings, and capability to respond
- (d) develop intelligence products to standard for response, seeking legal advice prior to release to the FCC
- (e) store correspondence in accordance with the department's record management policy.

Formatted: Normal, Pattern: Clear

Stored

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Disclosure

The FFC will initiate and facilitate information sharing, issuing RFIs via the DEWR Fraud Fusion Taskforce mailbox.

The Fraud Team through an intelligence led process may also initiate a release of information, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

Release of information will most typically be in the form of an email to the FFC mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce Officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?

This will depend on the number of persons or entities flagged as concerning.

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes

s 42(1)

s 42(1)

☒	The <u>scope</u> of the personal information being handled is new or different.
☒	The personal information is being handled in a new or different <u>context</u> .
☒	The <u>purpose</u> for which the personal information is being handled is new or different.
☒	The <u>risk</u> of handling the personal information is new or different.
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).	
You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	

Section 3: Likely impact on the privacy of individuals

s 42(1)

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:		Yes
☐	Handling large amounts of personal information.	
☒	Handling sensitive information ³ .	
☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.	

s 42(1)

☒	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☒	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

- ☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
- ☒ Using information for data matching or linking unconnected personal information.

s 42(1)

s 42(1)

If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.

If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:

Not applicable.

Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?

Yes

If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

s 42(1)

s 42(1)

A PIA is required as there are or potentially are high privacy risk elements

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by s 22(1) Assistant Secretary and Chief Internal Auditor

Date: 31/12/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence. The Taskforce along with the Taskforce's Fraud Fusion Centre (FFC) is operated, co-ordinated and led by the Australian Criminal Intelligence Commission (ACIC). The purpose of ACIC is 'to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence' (as set out under section 7A of the <i>Australian Crime Commission Act 2002</i>). This project is seeking a streamlined approach to the treatment and management of information sharing between the department and the FFC as noted in the Fraud Fusion Taskforce Memorandum of Understanding (MOU).
--	---

s 42(1)

s 42(1)

- (a) in response to a request for information initiated by the FFC, or
- (b) proactively – when information held by the department is considered to be within the remit of the Taskforce MOU.

	The department is not responsible for the type of information collected by the ACIC and shared to Taskforce partner agencies for data matching. The department will manage incoming data releases from the FFC in line with the Taskforce Data Governance Framework. The MOU notes: 1. The Taskforce seeks to understand, prevent, respond to and disrupt criminal activity against various government programs, including serious organised crime (SOC), by sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs. 2. The Taskforce seeks to enhance government co-ordination to prevent, detect, and respond to fraud and related criminal activity within and against government programs by collecting, correlating, analysing, and disseminating information and intelligence to develop appropriate responses to criminal activity, and fraud, including SOC. 3. The Fraud Fusion Intelligence Program will be established and independently managed by ACIC and oversee the activities of the FFC, including its administration, intelligence collection, development, and data sharing.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Compliance Intelligence Team FEG Program Management Office Assurance Insights Team Risk Management Insurance Incidents Team External Stakeholder/s: ACIC

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information ¹ ?			Yes			
- If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						
Type of information	Collect	Use	Disclose	Store	Destroy ²	De-identify
Names	☒	☐	☒	☒	☐	☐
Signatures	☐	☒	☒	☒	☐	☐
Addresses	☐	☒	☒	☒	☐	☐
Email addresses	☒	☒	☒	☒	☐	☐
Telephone numbers	☐	☒	☒	☒	☐	☐
Dates of birth	☐	☒	☒	☒	☐	☐
Sex or gender	☐	☒	☒	☒	☐	☐
Opinions or feedback	☐	☒	☐	☒	☐	☐
Commentary	☐	☒	☒	☒	☐	☐
CRNs or JSIDs	☐	☒	☒	☒	☐	☐
USIs or CHESSNs	☐	☒	☒	☒	☐	☐
Tax file numbers	☐	☒	☐	☒	☐	☐
Financial information	☐	☒	☒	☒	☐	☐
Bank account details	☐	☒	☒	☒	☐	☐
Identity documents	☐	☒	☒	☒	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

s 42(1)

Commented s 22(1) here is a technical issue 'ticking' boxes for 'Collect' column.

s 42(1)

s 42(1)

Commented s 22(1) This cannot be confirmed. The collection of, or disclosing of 'racial or ethnic origin' information is dependent on the scope of the investigation and significance this information may have on the investigation or operation. At best, the probability (or risk factor) of this information being needed is low, but cannot be wholly excluded.

Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/A						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?						
<i>You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.</i>						
Request For Information (RFI) received from the FCC may contain personal information of individuals and/or entities that have been approved for release under section 59AA of the <i>Australian Crime Commission Act 2002</i> (Cth) with the intention to generate intelligence and insights from partner agencies. <u>Information received from the FFC will include tactical and strategic intelligence products addressing criminal and risk indicate activity insights. These will be used to inform administrative data sharing and individual agency activity.</u> <u>It is the role of the ACIC to determine the type of information, including personal information, to be shared with partner agencies.</u>						
The department will collate personal information it holds in preparation for disclosure if requested by the FFC under an RFI or it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption. The department will manage incoming data requests by following practicable actions: (a) consult with the Taskforce on the scope of a RFI; its operational significance and required actions (in 28 days??) (b) inform the relevant delegate of the RFI (c) work with departmental business areas (primarily compliance areas) to identify department's information and data holdings, and capability to respond (d) develop intelligence products to standard for response, seeking legal advice prior to release to the FFC (e) store correspondence in accordance with the department's record management policy.						

s 42(1)

s 42(1)

Stored

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Disclosure

The FFC will initiate and facilitate information sharing, issuing RFIs via the DEWR Fraud Fusion Taskforce mailbox.

The Fraud Team through an intelligence led process may also initiate a release of information, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

Release of information will most typically be in the form of an email to the FFC mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce Officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?

This will depend on the number of persons or entities flagged as concerning.

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes

s 42(1)

☒	The <u>scope</u> of the personal information being handled is new or different.
☒	The personal information is being handled in a new or different <u>context</u> .
☒	The <u>purpose</u> for which the personal information is being handled is new or different.
☒	The <u>risk</u> of handling the personal information is new or different.
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).	
You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	

Section 3: Likely impact on the privacy of individuals

s 42(1)

s 42(1)

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	Yes
☐ Handling large amounts of personal information.	
☒ Handling sensitive information ³ .	
☐ Handling personal information in a way that is likely to raise public concern or unlikely to have	

s 42(1)

☒	agencies and/or contracted services providers.
☒	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

- ☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
- ☒ Using information for data matching or linking unconnected personal information.

s 42(1)

s 42(1)

- ☒ Handling personal information for activities of a long term or permanent duration.

If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.

If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:

Not applicable.

Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?

Yes

If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

s 42(1)

s 42(1)

A PIA is required as there are or potentially are high privacy risk elements

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

s 22(1)

Approved by _____, Assistant Secretary and Chief Internal Auditor

Date: 31/12/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).

Document 8 (page 51-57) deleted under section 42(1) of the *Freedom of Information Act 1982* (Cth).

Document 9 (page 58-64) deleted under section 42(1) of the *Freedom of Information Act 1982* (Cth).



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes

The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence.

The Taskforce along with the Taskforce's Fraud Fusion Centre (FFC) is operated, co-ordinated and led by the Australian Criminal Intelligence Commission (ACIC).

The purpose of ACIC is 'to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence' (as set out under section 7A of the *Australian Crime Commission Act 2002*).

This project is seeking a streamlined approach to the treatment and management of information sharing between the department and the FFC as noted in the Fraud Fusion Taskforce Memorandum of Understanding (MOU).

s 42(1)

- (a) in response to a request for information initiated by the FFC, or
- (b) proactively – when information held by the department is considered to be within the remit of the Taskforce MOU.

ACIC may provide personal information to the department for data matching purposes. The department is not responsible for the type

s 42(1)

	of information collected by the ACIC and shared to Taskforce partner agencies for data matching. The department will manage incoming data releases from the FFC in line with the Taskforce Data Governance Framework. The MOU notes: 1. The Taskforce seeks to understand, prevent, respond to and disrupt criminal activity against various government programs, including serious organised crime (SOC), by sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs. 2. The Taskforce seeks to enhance government co-ordination to prevent, detect, and respond to fraud and related criminal activity within and against government programs by collecting, correlating, analysing, and disseminating information and intelligence to develop appropriate responses to criminal activity, and fraud, including SOC. 3. The Fraud Fusion Intelligence Program will be established and independently managed by ACIC and oversee the activities of the FFC, including its administration, intelligence collection, development, and data sharing.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Compliance Intelligence Team FEG Program Management Office Assurance Insights Team Risk Management Insurance Incidents Team External Stakeholder/s: ACIC

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information ¹ ?			Yes			
- If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						
Type of information	Collect	Disclose	Store	Destroy ²	De-identify	
Names	☒	☒	☒	☒	☐	
Signatures	☐	☒	☒	☒	☐	
Addresses	☐	☒	☒	☒	☐	
Email addresses	☒	☒	☒	☒	☐	
Telephone numbers	☐	☒	☒	☒	☐	
Dates of birth	☐	☒	☒	☒	☐	
Sex or gender	☐	☒	☒	☒	☐	
Opinions or feedback	☐	☒	☐	☒	☐	
Commentary	☐	☒	☒	☒	☐	
CRNs or JSIDs	☐	☒	☒	☒	☐	
USIs or CHESSNs	☐	☒	☒	☒	☐	
Tax file numbers	☐	☒	☐	☒	☐	
Financial information	☐	☒	☒	☒	☐	
Bank account details	☐	☒	☒	☒	☐	
Identity documents	☐	☒	☒	☒	☐	
Political opinions	☐	☐	☐	☐	☐	
Membership of a political association	☐	☐	☐	☐	☐	
Religious beliefs or affiliations	☐	☐	☐	☐	☐	
Philosophical beliefs	☐	☐	☐	☐	☐	
Memberships of a trade union	☐	☐	☐	☐	☐	
Sexual orientation or practices	☐	☐	☐	☐	☐	

s 42(1)

Commented s 22(1) here is a technical issue 'ticking' boxes for 'Collect' column.

s 42(1)

s 42(1)

Commented s 22(1) This cannot be confirmed. The collection of, or disclosing of 'racial or ethnic origin' information is dependent on the scope of the investigation and significance this information may have on the investigation or operation. At best, the probability (or risk factor) of this information being needed is low, but cannot be wholly excluded.

s 42(1)

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐

If not listed above, specify other type/s of personal information handled in the project or initiative:

N/A

How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?

You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.

s 42(1)

s 42(1)

Request For Information (RFI) received from the FCC may contain personal information of individuals and/or entities that have been approved for release under section 59AA of the *Australian Crime Commission Act 2002* (Cth) with the intention to generate intelligence and insights from partner agencies.

Information received from the FCC will include tactical and strategic intelligence products addressing criminal and risk indicate activity insights. These will be used to inform administrative data sharing and individual agency activity.

It is the role of the ACIC to determine the type of information, including personal information, to be shared with partner agencies.

s 42(1)

s 42(1)

The department will collate personal information it holds in preparation for disclosure if requested by the FCC under an RFI or it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

The department will manage incoming data requests by following practicable actions:

- (a) consult with the Taskforce on the scope of a RFI; its operational significance and required actions (in 28 days)
- (b) inform the relevant delegate of the RFI
- (c) work with departmental business areas (primarily compliance areas) to identify department's information and data holdings, and capability to respond
- (d) develop intelligence products to standard for response, seeking legal advice prior to release to the FCC
- (e) store correspondence in accordance with the department's record management policy.

Stored

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Disclosure

The FFC will initiate and facilitate information sharing, issuing RFIs via the DEWR Fraud Fusion Taskforce mailbox.

The Fraud Team through an intelligence led process may also initiate a release of information, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

Release of information will most typically be in the form of an email to the FFC mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce Officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?

This will depend on the number of persons or entities flagged as concerning.

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes

s 42(1)

☒	The <u>scope</u> of the personal information being handled is new or different.
☒	The personal information is being handled in a new or different <u>context</u> .
☒	The <u>purpose</u> for which the personal information is being handled is new or different.
☒	The <u>risk</u> of handling the personal information is new or different.
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).	
You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	

Section 3: Likely impact on the privacy of individuals

s 42(1)

s 42(1)

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	Yes
☐ Handling large amounts of personal information.	
☒ Handling sensitive information ³ .	
☐ Handling personal information in a way that is likely to raise public concern or unlikely to have community support.	

s 42(1)

☒	agencies and/or contracted services providers.
☒	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

- ☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
- ☒ Using information for data matching or linking unconnected personal information.

s 42(1)

s 42(1)

- ☒ Handling personal information for activities of a long term or permanent duration.

If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.

If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:

Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?

Yes

If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

s 42(1)

s 42(1)

A PIA is required as there are or potentially are high privacy risk elements

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: s 22(1) Assistant Secretary and Chief Internal Auditor

Date: 31/12/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes

The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence.

The Taskforce along with the Taskforce's Fraud Fusion Centre (FFC) is operated, co-ordinated and led by the Australian Criminal Intelligence Commission (ACIC).

The purpose of ACIC is 'to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence' (as set out under section 7A of the *Australian Crime Commission Act 2002*).

This project is seeking a streamlined approach to the treatment and management of information sharing between the department and the FFC as noted in the Fraud Fusion Taskforce Memorandum of Understanding (MOU).

s 42(1)

FFC, or
(b) proactively – when information held by the department is considered to be within the remit of the Taskforce MOU.

ACIC may provide personal information to the department for data matching purposes. The department is not responsible for the type

s 42(1)

	of information collected by the ACIC and shared to Taskforce partner agencies for data matching. The department will manage incoming data releases from the FFC in line with the Taskforce Data Governance Framework. The MOU notes: 1. The Taskforce seeks to understand, prevent, respond to and disrupt criminal activity against various government programs, including serious organised crime (SOC), by sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs. 2. The Taskforce seeks to enhance government co-ordination to prevent, detect, and respond to fraud and related criminal activity within and against government programs by collecting, correlating, analysing, and disseminating information and intelligence to develop appropriate responses to criminal activity, and fraud, including SOC. 3. The Fraud Fusion Intelligence Program will be established and independently managed by ACIC and oversee the activities of the FFC, including its administration, intelligence collection, development, and data sharing.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Compliance Intelligence Team FEG Program Management Office Assurance Insights Team Risk Management Insurance Incidents Team External Stakeholder/s: ACIC

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information ¹ ?			Yes			
- If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						
Type of information	s 42(1)		Disclose	Store	Destroy ²	De-identify
Names	☒	☒	☒	☒	☐	☐
Signatures	☐	☒	☒	☒	☐	☐
Addresses	☐	☒	☒	☒	☐	☐
Email addresses	☒	☒	☒	☒	☐	☐
Telephone numbers	☐	☒	☒	☒	☐	☐
Dates of birth	☐	☒	☒	☒	☐	☐
Sex or gender	☐	☒	☒	☒	☐	☐
Opinions or feedback	☐	☒	☐	☒	☐	☐
Commentary	☐	☒	☒	☒	☐	☐
CRNs or JSIDs	☐	☒	☒	☒	☐	☐
USIs or CHESSNs	☐	☒	☒	☒	☐	☐
Tax file numbers	☐	☒	☐	☒	☐	☐
Financial information	☐	☒	☒	☒	☐	☐
Bank account details	☐	☒	☒	☒	☐	☐
Identity documents	☐	☒	☒	☒	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

s 42(1)

Commented s 22(1) There is a technical issue 'ticking' boxes for 'Collect' column.

s 42(1)

s 42(1)

Commented s 22(1) This cannot be confirmed. The collection of, or disclosing of 'racial or ethnic origin' information is dependent on the scope of the investigation and significance this information may have on the investigation or operation. At best, the probability (or risk factor) of this information being needed is low, but cannot be wholly excluded.

s 42(1)

Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐

If not listed above, specify other type/s of personal information handled in the project or initiative:

N/A

How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?

You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.

s 42(1)

Request For Information (RFI) received from the FCC may contain personal information of individuals and/or entities that have been approved for release under section 59AA of the *Australian Crime Commission Act 2002* (Cth) with the intention to generate intelligence and insights from partner agencies.

Information received from the FCC will include tactical and strategic intelligence products addressing criminal and risk indicate activity insights. These will be used to inform administrative data sharing and individual agency activity.

It is the role of the ACIC to determine the type of information, including personal information, to be shared with partner agencies.

s 42(1)

The department will collate personal information it holds in preparation for disclosure if requested by the FCC under an RFI or it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

The department will manage incoming data requests by following practicable actions:

- (a) consult with the Taskforce on the scope of a RFI; its operational significance and required actions (in 28 days)
- (b) inform the relevant delegate of the RFI
- (c) work with departmental business areas (primarily compliance areas) to identify department's information and data holdings, and capability to respond
- (d) develop intelligence products to standard for response, seeking legal advice prior to release to the FCC
- (e) store correspondence in accordance with the department's record management policy.

s 42(1)

s 42(1)

Stored

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Disclosure

The FFC will initiate and facilitate information sharing, issuing RFIs via the DEWR Fraud Fusion Taskforce mailbox.

The Fraud Team through an intelligence led process may also initiate a release of information, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

Release of information will most typically be in the form of an email to the FFC mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce Officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?

This will depend on the number of persons or entities flagged as concerning.

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes

s 42(1)

s 42(1)

☒	The <u>scope</u> of the personal information being handled is new or different.
☒	The personal information is being handled in a new or different <u>context</u> .
☒	The <u>purpose</u> for which the personal information is being handled is new or different.
☒	The <u>risk</u> of handling the personal information is new or different.
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).	
You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	

Section 3: Likely impact on the privacy of individuals

s 42(1)

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:		Yes
☐	Handling large amounts of personal information.	
☒	Handling sensitive information ³ .	
☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.	
☒	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.	
☒	Using or disclosing personal information for profiling or behavioural predictions.	
☐	Using personal information for automated decision-making.	
☐	Collecting personal information through systematic monitoring or tracking of individuals.	

s 42(1)

s 42(1)

s 42(1)

s 42(1)

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

☒	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☒	Using information for data matching or linking unconnected personal information.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	
	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

s 42(1)

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

s 42(1)

s 42(1)

	A PIA is required as there are or potentially are high privacy risk elements
--	--

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: s 22(1) Assistant Secretary and Chief Internal Auditor

Date: 31/12/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence. The Taskforce along with the Taskforce's Fraud Fusion Centre (FFC) is operated, co-ordinated and led by the Australian Criminal Intelligence Commission (ACIC). The purpose of ACIC is 'to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence' (as set out under section 7A of the <i>Australian Crime Commission Act 2002</i>). This project is seeking a streamlined approach to the treatment and management of information sharing between the department and the FFC as noted in the Fraud Fusion Taskforce Memorandum of Understanding (MOU). s 42(1) (a) in response to a request for information initiated by the FFC, or (b) proactively – when information held by the department is considered to be within the remit of the Taskforce MOU. ACIC may provide personal information to the department for data matching purposes. The department is not responsible for the type
--	--

s 42(1)

	of information collected by the ACIC and shared to Taskforce partner agencies for data matching. The department will manage incoming data releases from the FFC in line with the Taskforce Data Governance Framework. The MOU notes: 1. The Taskforce seeks to understand, prevent, respond to and disrupt criminal activity against various government programs, including serious organised crime (SOC), by sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs. 2. The Taskforce seeks to enhance government co-ordination to prevent, detect, and respond to fraud and related criminal activity within and against government programs by collecting, correlating, analysing, and disseminating information and intelligence to develop appropriate responses to criminal activity, and fraud, including SOC. 3. The Fraud Fusion Intelligence Program will be established and independently managed by ACIC and oversee the activities of the FFC, including its administration, intelligence collection, development, and data sharing.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Compliance Intelligence Team FEG Program Management Office Assurance Insights Team Risk Management Insurance Incidents Team External Stakeholder/s: ACIC

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹?

- If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below.
- If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.

Yes

s 42(1)

			Disclose	Store	Destroy ²	De-identify
Names	☒	☒	☒	☒	☐	☐
Signatures	☐	☒	☒	☒	☐	☐
Addresses	☐	☒	☒	☒	☐	☐
Email addresses	☒	☒	☒	☒	☐	☐
Telephone numbers	☐	☒	☒	☒	☐	☐
Dates of birth	☐	☒	☒	☒	☐	☐
Sex or gender	☐	☒	☒	☒	☐	☐
Opinions or feedback	☐	☒	☐	☒	☐	☐
Commentary	☐	☒	☒	☒	☐	☐
CRNs or JSIDs	☐	☒	☒	☒	☐	☐
USIs or CHESSNs	☐	☒	☒	☒	☐	☐
Tax file numbers	☐	☒	☐	☒	☐	☐
Financial information	☐	☒	☒	☒	☐	☐
Bank account details	☐	☒	☒	☒	☐	☐
Identity documents	☐	☒	☒	☒	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐

s 42(1)

Commented s 22(1) There is a technical issue 'ticking' boxes for 'Collect' column.

s 42(1)

s 42(1)

Commented s 22(1) This cannot be confirmed. The collection of, or disclosing of 'racial or ethnic origin' information is dependent on the scope of the investigation and significance this information may have on the investigation or operation. At best, the probability (or risk factor) of this information being needed is low, but cannot be wholly excluded.

s 42(1)

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐

If not listed above, specify other type/s of personal information handled in the project or initiative:

N/A

How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?

You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.

s 42(1)

s 42(1)

Request For Information (RFI) received from the FCC may contain personal information of individuals and/or entities that have been approved for release under section 59AA of the *Australian Crime Commission Act 2002* (Cth) with the intention to generate intelligence and insights from partner agencies.

Information received from the FFC will include tactical and strategic intelligence products addressing criminal and risk indicate activity insights. These will be used to inform administrative data sharing and individual agency activity.

It is the role of the ACIC to determine the type of information, including personal information, to be shared with partner agencies.

s 42(1)

s 42(1)

The department will collate personal information it holds in preparation for disclosure if requested by the FFC under an RFI or it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

The department will manage incoming data requests by following practicable actions:

- (a) consult with the Taskforce on the scope of a RFI; its operational significance and required actions (in 28 days)
- (b) inform the relevant delegate of the RFI
- (c) work with departmental business areas (primarily compliance areas) to identify department's information and data holdings, and capability to respond
- (d) develop intelligence products to standard for response, seeking legal advice prior to release to the FFC
- (e) store correspondence in accordance with the department's record management policy.

Stored

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Disclosure

The FFC will initiate and facilitate information sharing, issuing RFIs via the DEWR Fraud Fusion Taskforce mailbox.

The Fraud Team through an intelligence led process may also initiate a release of information, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

Release of information will most typically be in the form of an email to the FFC mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce Officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?

This will depend on the number of persons or entities flagged as concerning.

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes

s 42(1)

s 42(1)

☒	The <u>scope</u> of the personal information being handled is new or different.
☒	The personal information is being handled in a new or different <u>context</u> .
☒	The <u>purpose</u> for which the personal information is being handled is new or different.
☒	The <u>risk</u> of handling the personal information is new or different.
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).	
You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	

Section 3: Likely impact on the privacy of individuals

s 42(1)

	Yes
To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	
☐	Handling large amounts of personal information.
☒	Handling sensitive information ³ .
☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.

s 42(1)

☒	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☒	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

s 42(1)

☒	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☒	Using information for data matching or linking unconnected personal information.

s 42(1)

s 42(1)

☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	
	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

s 42(1)

s 42(1)

	A PIA is required as there are or potentially are high privacy risk elements
--	--

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: s 22(1) ssistant Secretary and Chief Internal Auditor

Date: ~~31/12/2023~~ 31/01/2024

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Australian Government
Department of Employment
and Workplace Relations

Privacy Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes

The Fraud Fusion Taskforce (the Taskforce) has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence.

The Taskforce along with the Taskforce's Fraud Fusion Centre (FFC) is operated, co-ordinated and led by the Australian Criminal Intelligence Commission (ACIC).

The purpose of ACIC is 'to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence' (as set out under section 7A of the *Australian Crime Commission Act 2002*).

This project is seeking a streamlined approach to the treatment and management of information sharing between the department and the FFC as noted in the Fraud Fusion Taskforce Memorandum of Understanding (MOU).

The department may release information in one of two ways:

- (a) in response to a request for information initiated by the FFC, or
- (b) proactively – when information held by the department is considered to be within the remit of the Taskforce MOU.

ACIC may provide personal information to the department for data matching purposes. The department is not responsible for the type

	of information collected by the ACIC and shared to Taskforce partner agencies for data matching. The department will manage incoming data releases from the FFC in line with the Taskforce Data Governance Framework. The MOU notes: 1. The Taskforce seeks to understand, prevent, respond to and disrupt criminal activity against various government programs, including serious organised crime (SOC), by sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs. 2. The Taskforce seeks to enhance government co-ordination to prevent, detect, and respond to fraud and related criminal activity within and against government programs by collecting, correlating, analysing, and disseminating information and intelligence to develop appropriate responses to criminal activity, and fraud, including SOC. 3. The Fraud Fusion Intelligence Program will be established and independently managed by ACIC and oversee the activities of the FFC, including its administration, intelligence collection, development, and data sharing.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Compliance Intelligence Team FEG Program Management Office Assurance Insights Team Risk Management Insurance Incidents Team External Stakeholder/s: ACIC

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information ¹ ?						Yes	
- If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.							
Type of information	Collect	Use	Disclose	Store	Destroy ²	De-identify	
Names	☒	☒	☒	☒	☐	☐	
Signatures	☐	☒	☒	☒	☐	☐	
Addresses	☐	☒	☒	☒	☐	☐	
Email addresses	☒	☒	☒	☒	☐	☐	
Telephone numbers	☐	☒	☒	☒	☐	☐	
Dates of birth	☐	☒	☒	☒	☐	☐	
Sex or gender	☐	☒	☒	☒	☐	☐	
Opinions or feedback	☐	☒	☐	☒	☐	☐	
Commentary	☐	☒	☒	☒	☐	☐	
CRNs or JSIDs	☐	☒	☒	☒	☐	☐	
USIs or CHESSNs	☐	☒	☒	☒	☐	☐	
Tax file numbers	☐	☒	☐	☒	☐	☐	
Financial information	☐	☒	☒	☒	☐	☐	
Bank account details	☐	☒	☒	☒	☐	☐	
Identity documents	☐	☒	☒	☒	☐	☐	
Racial or ethnic origin	☐	☐	☐	☐	☐	☐	
Political opinions	☐	☐	☐	☐	☐	☐	
Membership of a political association	☐	☐	☐	☐	☐	☐	
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐	
Philosophical beliefs	☐	☐	☐	☐	☐	☐	
Memberships of a trade union	☐	☐	☐	☐	☐	☐	
Sexual orientation or practices	☐	☐	☐	☐	☐	☐	

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/A						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative? <i>You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.</i>						
<u>Collection</u> Request For Information (RFI) received from the FCC may contain personal information of individuals and/or entities that have been approved for release under section 59AA of the <i>Australian Crime Commission Act 2002</i> (Cth) with the intention to generate intelligence and insights from partner agencies. Information received from the FFC will include tactical and strategic intelligence products addressing criminal and risk indicate activity insights. These will be used to inform administrative data sharing and individual agency activity. It is the role of the ACIC to determine the type of information, including personal information, to be shared with partner agencies. <u>Use</u> The department will collate personal information it holds in preparation for disclosure if requested by the FFC under an RFI or it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption. The department will manage incoming data requests by following practicable actions: (a) consult with the Taskforce on the scope of a RFI; its operational significance and required actions (in 28 days) (b) inform the relevant delegate of the RFI (c) work with departmental business areas (primarily compliance areas) to identify department's information and data holdings, and capability to respond (d) develop intelligence products to standard for response, seeking legal advice prior to release to the FFC (e) store correspondence in accordance with the department's record management policy.						

Stored

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

Disclosure

The FFC will initiate and facilitate information sharing, issuing RFIs via the DEWR Fraud Fusion Taskforce mailbox.

The Fraud Team through an intelligence led process may also initiate a release of information, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption.

Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

Release of information will most typically be in the form of an email to the FFC mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce Officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?

This will depend on the number of persons or entities flagged as concerning.

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes



The nature or type of the personal information being handled is new or different.

☒	The <u>scope</u> of the personal information being handled is new or different.
☒	The personal information is being handled in a new or different <u>context</u> .
☒	The <u>purpose</u> for which the personal information is being handled is new or different.
☒	The <u>risk</u> of handling the personal information is new or different.
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s). You should provide the name of the same or similar project or initiative <u>where the practice(s) have been assessed previously</u> and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals? To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	Yes
☐ Handling large amounts of personal information.	
☒ Handling sensitive information ³ .	
☐ Handling personal information in a way that is likely to raise public concern or unlikely to have community support.	
☒ Handling the personal information of individuals who are vulnerable. ⁴	
☒ Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.	
☒ Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.	
☒ Using or disclosing personal information for profiling or behavioural predictions.	
☐ Using personal information for automated decision-making.	
☐ Collecting personal information through systematic monitoring or tracking of individuals.	

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

☒	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☒	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	
Yes	
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	A PIA is required as there are or potentially are high privacy risk elements
---------	--

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: ^{s 22(1)} Assistant Secretary and Chief Internal Auditor

Date: 3/01/2024

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Australian Government
Department of Employment
and Workplace Relations

Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code). This assessment should be completed after reading the PIA policy located [here](#).

Project or initiative

The PTA is an addendum to the previous Fraud Fusion Centre (FFC) – data sharing project's PTA and the approved PIA, signed 4 May 2024.

The addendum is to expand on the approach to the treatment and management of information sharing between the Department of Employment and Workplace Relations (DEWR), the Fraud Fusion Taskforce (Taskforce) and its Partners for Taskforce special operation/s (also known as Strikeforce/s) and/or project/s.

The Taskforce is jointly lead and operated by the National Disability Insurance Agency (NDIA) and Services Australia (SA) to prevent, detect and disrupt serious fraud. The Taskforce will enable intelligence sharing, identification and response by its Partners to identify and address fraud perpetrated by Serious and Organised Crime (SOC) entities and others seeking to exploit the Government's programs.

Special Strikeforce operation/s or project/s may be led by either the NDIA, SA or one of the Taskforce Partners. The lead will be determined on a case-by-case basis by the FFT Governance Framework – such as the FFT Operational Working Group, FFT Intelligence and Operations Committee or FFT Inter-Departmental Committee.

Brief project or initiative
description and intended
goals/outcomes

Commented ^{s 22(1)} Completing the privacy threshold assessment is the responsibility of the area that has the functions in relation to the project/initiative. The area needs to satisfy themselves as to the accuracy of the information in this assessment and will be the owner of this assessment.

This assessment may be provided to the Office of the Australian Information Commissioner as evidence of the consideration given to whether a PIA is required, and therefore the information needs to be detailed and correct.

This assessment should be completed before the project or initiative commences.

Commented ^{s 22(1)} You should include sufficient detail such that someone who has no background can understand what the project or initiative involves. The description should be drafted in a way that it could be clearly understood on its face by a member of the public.

If you are going to use an acronym ensure you spell the word out in full first time.

Avoid technical jargon.

The lead Partner of these operation/s or project/s may determine to release, or request information from FFT partner agencies, the lead Partner will follow the Taskforces Memorandum of Understanding (MOU).

The MOU outlines the Taskforce purpose, its strategic focus, Governance and Responsibilities and how data, information sharing and security is to be handled by each Partner.

Clause 5 – Taskforce Purpose, paragraph 2 outlines the FFTs:

- a) strategic focus on:
 - 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.**

Clause 5 – Taskforce Purpose, paragraph 3 outlines how the FFT:

- a) will 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 Clause 7 – Governance and Responsibilities - provides an overview of the agreed to operational conditions and management of the Taskforce. Clause 14 – Data, information sharing and security - provides the framework and management on how each Partner will manage the sharing of data and information, its security and disclosure.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Enterprise Risk, Assurance and Investigations Branch, Legal and Assurance Division, DEWR Compliance Intelligence, Skills Program Compliance Branch, Skills and Training Group, DEWR

Commented s 22(1) Identify internal stakeholders at the Team/Branch/Division level.

	FEG Program Management Office, Entitlements Safeguards Division, Workplace Relations Group, DEWR Assurance Insights, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR Risk Management Insurance Incidents, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR External Stakeholder/s: Any and all current and future FFT Partners.
--	--

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.					Yes	
Type of information	Collect	Use	Disclose	Store		
Names	☐	☒	☒	☐	☐	☐
Signatures	☐	☒	☒	☐	☐	☐
Addresses	☐	☒	☒	☐	☐	☐
Email addresses	☐	☒	☒	☐	☐	☐
Telephone numbers	☐	☒	☒	☐	☐	☐
Dates of birth	☐	☒	☒	☐	☐	☐
Sex or gender	☐	☒	☒	☐	☐	☐
Opinions or feedback	☐	☒	☒	☐	☐	☐
Commentary	☐	☒	☒	☐	☐	☐
CRNs or JSIDs	☐	☒	☒	☐	☐	☐
USIs or CHESSNs	☐	☒	☒	☐	☐	☐
Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☐	☒	☒	☐	☐	☐
Bank account details	☐	☒	☒	☐	☐	☐

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Identity documents	☐	☒	☒	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Partnership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Partnerships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☒	☒	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/A						
How will personal information be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?						
You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.						
The DEWR FFT team will be the central point of contact for all requests and release of information.						
Information Sharing No information will be requested from individuals directly associated with DEWR programs, all information gathered will be via DEWR's already established data holdings e.g., ESS, ADMS, TYIMS, FEG, ESS Tip-off and iBase etc. Additional information may be sourced through paid third parties e.g., Equifax or open source such as ABN lookup or Google. The lead agency may initiate and facilitate information sharing, by: <u>Public Interest Certificate (PIC) or Clapoom</u>						

Commented S 22(1) : Please ensure you include the following detail

- Where the personal information will be stored
- Who will have access to the personal information, including any access by cloud or software providers
- If personal information will be disclosed to a third party, how the personal information will be shared (eg by email or Secure File Transfer Protocol)
- If personal information will be stored on the cloud, whether the servers are located in Australia or overseas

- a) any release of information from the lead agency to DEWR will be the responsibility of the lead agency to ensure they met and adhered to any relevant legislation and data policy (of their department and FFT MOU) to release the information to the other FFT Partners.

The lead agency releasing information may request data from DEWR to enable the FFT meet its strategic purposes. The information requested will be but not limited to:

- Previous or current compliance or fraud activities against certain organisations or individuals,
- Contact details of individuals,
- Bank account details, etc.

Request for Information (RFI)

- b) the lead agency may request DEWR FFT review its data holdings and provide specific information about companies, people and payments. The information requested will be but not limited to:

- Previous or current compliance or fraud activities against certain organisations or individuals,
- Contact details of individuals,
- Bank account details, etc.

DEWR Release of Information

DEWR FFT team through an intelligence led process may release information, proactively or as per a RFI, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption. The lead agency may then release this information to other FFT Partners.

The nature of information collected and released may vary depending on the type or request, we believe the information will fall within these categories:

- (a) material that is both personal and protected information;
- (b) material that is personal but not protected information; and
- (c) material that is neither personal nor protected information (where the information has not been obtained under any law and relates to a business or person).

Storage

DEWR

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

FFT Partner agencies

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

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

Disclosure

Information collected and prepared for disclosure to the Taskforce and its Partners will be in accordance with appropriate legislation and clearance from the Information Legal Team (ILT). Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

DEWR intends to add restrictions to the release of information with the following wording:

The information is disclosed to the <INSERT DEPT> being a Commonwealth authority, as DEWR is satisfied it is necessary in order to enable or assist your agency/department to perform or exercise its powers or functions. Any further sharing of this information beyond the <INSERT DEPT> is to be approved by DEWR.

It is anticipated any release of information from DEWR to the Taskforce and its Partners will be either via DEWRs established CLAPOOM or PIC processes.

Release of information will most typically be in the form of an email from the FFT mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?	This will depend on the number of
---	-----------------------------------

	persons or entities flagged as concerning. (TBC)
--	--

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?	
If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.	Yes
☐ The <u>nature or type</u> of the personal information being handled is new or different.	
☐ The <u>scope</u> of the personal information being handled is new or different.	
☐ The personal information is being handled in a new or different <u>context</u> .	
☐ The <u>purpose</u> for which the personal information is being handled is new or different.	
☒ The <u>risk</u> of handling the personal information is new or different.	
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s)	
You should provide the name of the same or similar project or initiative <u>where the practice(s) have been assessed previously</u> and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	
N/A	

Commented s 22(1) There is a new or changed way of handling personal information if any of the following apply:

- The handling relates to a completely new function or activity
- The department will be collecting more personal information than it used to or initiating a new collection
- The department will be using or disclosing the personal information for a different purpose than previously, including movement from paper based to electronic
- The department will be disclosing personal information to a third party that has not previously been disclosed
- A change is being made to how the personal information will be stored or disclosed
- A change is being made to who will have access to the personal information

Commented s 22(1) There needs to be more in common than just the means of handling (eg by email) for this to apply.

In addition, a privacy threshold assessment must have already been completed for the existing practice the handling is being compared to.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?	
To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	Choose an item.
☒ Handling large amounts of personal information.	
☒ Handling sensitive information ³ .	

Commented s 22(1) Whether a project or initiative is likely to have a significant impact on privacy depends on a range of factors.

The more of the factors below that apply the more likely the project or initiative is to have a significant impact on privacy. This includes if a security assessment has given the project or initiative a medium or high risk rating it should be considered as being likely to have a significant impact on privacy.

Commented s 22(1) This factor encompasses consideration of both the number of individuals whose personal information is being handled, the volume of personal information about those individuals, and the number of people internally and externally who have access to that personal information.

³ 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

☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
☐	Handling the personal information of individuals who are vulnerable. ⁴
☐	Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
☒	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☐	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.
☐	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☐	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
N/A	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
N/A	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	
Yes	
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	
N/A	

Commented ^s 22(1) : This factor requires consideration of the potential consequences for the individual in the handling, and any potential mishandling, of their personal information. For example, if bank account details are involved there is the potential for financial loss from unauthorised access.

Commented ^s 22(1) This factor will apply if the project or initiative will be running for more than 3 months.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

Outcome	A PIA is required as there are or potentially are high privacy risk elements
---------	--

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: [Name/signature of Assistant Secretary or higher]

Date: Click or tap to enter a date.

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Australian Government
Department of Employment
and Workplace Relations

Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code). This assessment should be completed after reading the PIA policy located [here](#).

Project or initiative

The PTA is an addendum to the previous Fraud Fusion Centre (FFC) – data sharing project's PTA and the approved PIA, signed 4 May 2024.

The addendum is to expand on the approach to the treatment and management of information sharing between the Department of Employment and Workplace Relations (DEWR), the Fraud Fusion Taskforce (Taskforce) and its Partners for Taskforce-~~approved~~ ~~special~~ operation/s (also known as Strikeforce/s) and/or project/s.

The Taskforce is jointly lead and operated by the National Disability Insurance Agency (NDIA) and Services Australia (SA) to prevent, detect and disrupt [criminal exploitation of its programs and across the Commonwealth?](#) serious fraud. The Taskforce will enable intelligence sharing, identification and response by its Partners to identify and address fraud [vulnerabilities and fraud-related activities](#) perpetrated by Serious and Organised Crime (SOC) entities and others seeking to exploit the Government's programs.

~~Special Strikeforce o~~Operation/s or project/s may be led by either the NDIA, SA or one of the Taskforce Partners. The lead will be determined on a case-by-case basis by the FFT Governance Framework – such as the FFT Operational Working Group, FFT Intelligence and Operations Committee or FFT Inter-Departmental [Committee](#).

Brief project or initiative
description and intended
goals/outcomes

Commented s 22(1) completing the privacy threshold assessment is the responsibility of the area that has the functions in relation to the project/initiative. The area needs to satisfy themselves as to the accuracy of the information in this assessment and will be the owner of this assessment.

This assessment may be provided to the Office of the Australian Information Commissioner as evidence of the consideration given to whether a PIA is required, and therefore the information needs to be detailed and correct.

This assessment should be completed before the project or initiative commences.

Commented s 22(1) I think all Operations are approved by the IDC only??

Commented s 22(1) Could say here.. 'the FFT Governance Framework presided by the FFT Inter-Departmental Committee.' Thoughts??

Commented s 22(1) : You should include sufficient detail such that someone who has no background can understand what the project or initiative involves. The description should be drafted in a way that it could be clearly understood on its face by a member of the public.

If you are going to use an acronym ensure you spell the word out in full first time.

Avoid technical jargon.

The lead Partner of these operation/s or project/s may determine to release, or request information from FFT partner agencies; the lead Partner will follow the Taskforces Memorandum of Understanding (MOU).

The MOU outlines the Taskforce purpose, its strategic focus, Governance and Responsibilities and how data, information sharing and security is to be handled by each Partner.

Clause 5 – Taskforce Purpose, paragraph 2 outlines the FFT's:

- a) strategic focus on:
 - 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.**

Clause 5 – Taskforce Purpose, paragraph 34 outlines how the FFT:

- a) will 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 Clause 7 – Governance and Responsibilities - provides an overview of the agreed to operational conditions and management of the Taskforce. Clause 14 – Data, information sharing and security - provides the framework and management on how each Partner will manage the sharing of data and information, its security and disclosure.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Enterprise Risk, Assurance and Investigations Branch, Legal and Assurance Division, DEWR
	Compliance Intelligence, Skills Program Compliance Branch, Skills and Training Group, DEWR

Commented S 22/11 Do we need to add s11C(1)(a) s11C(1)(a) ind/or here??

Commented S 22/11 Identify internal stakeholders at the Team/Branch/Division level.

	FEG Program Management Office, Entitlements Safeguards Division, Workplace Relations Group, DEWR Assurance Insights, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR Risk Management Insurance Incidents, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR External Stakeholder/s: Any and all current and future FFT Partners.
--	--

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.					Yes	
Type of information	Collect	Use	Disclose	Store		
Names	☐	☒	☒	☐	☐	☐
Signatures	☐	☒	☒	☐	☐	☐
Addresses	☐	☒	☒	☐	☐	☐
Email addresses	☐	☒	☒	☐	☐	☐
Telephone numbers	☐	☒	☒	☐	☐	☐
Dates of birth	☐	☒	☒	☐	☐	☐
Sex or gender	☐	☒	☒	☐	☐	☐
Opinions or feedback	☐	☒	☒	☐	☐	☐
Commentary	☐	☒	☒	☐	☐	☐
CRNs or JSIDs	☐	☒	☒	☐	☐	☐
USIs or CHESSNs	☐	☒	☒	☐	☐	☐
Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☐	☒	☒	☐	☐	☐
Bank account details	☐	☒	☒	☐	☐	☐

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Identity documents	☐	☒	☒	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Partnership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Partnerships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☒	☒	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/A						
How will personal information be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?						
You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.						
The DEWR FFT team will be the central point of contact for all requests and release of information.						
Information Sharing No information will be requested from individuals directly associated with DEWR programs, all information gathered will be via DEWR's already established data holdings e.g., ESS, ADMS, TYIMS, FEG, ESS Tip-off and iBase etc. Additional information may be sourced through paid third parties e.g., Equifax or open source such as ABN lookup or Google. The lead agency may initiate and facilitate information sharing, by: <u>Public Interest Certificate (PIC) or CLAPOOM</u>						

Commented 22/11 : Please ensure you include the following details:

- Where the personal information will be stored
- Who will have access to the personal information, including any access by cloud or software providers
- If personal information will be disclosed to a third party, how the personal information will be shared (eg by email or Secure File Transfer Protocol)
- If personal information will be stored on the cloud, whether the servers are located in Australia or overseas

- a) any release of information from the lead agency to DEWR will be the responsibility of the lead agency to ensure they met and adhered to any relevant legislation and data policy (of their department and FFT MOU) to release the information to the other FFT Partners.

The lead agency releasing information may request data from DEWR to enable the FFT meet its strategic purposes. The information requested will be but not limited to:

- Previous or current compliance or fraud activities against certain organisations or individuals,
- Contact details of individuals,
- Bank account details, etc.

Request for Information (RFI)

- b) the lead agency may request DEWR FFT review its data holdings and provide specific information about companies, people and payments. The information requested will be but not limited to:

- Previous or current compliance or fraud activities against certain organisations or individuals,
- Contact details of individuals,
- Bank account details, etc.

DEWR Release of Information

DEWR FFT team through an intelligence led process may release information, proactively or as per a RFI, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption. The lead agency may then release this information to other FFT Partners.

The nature of information collected and released may vary depending on the type or (of?) request, we believe the information will fall within these categories:

- (a) material that is both personal and protected information;
- (b) material that is personal but not protected information; and
- (c) material that is neither personal nor protected information (where the information has not been obtained under any law and relates to a business or person).

Storage

Commented ^S 22(1) Could add here instead: 'being consistent with legislative obligations and agreements or arrangements relating to data management and the release of the information to the other FFT Partners'.

Commented ^S 22(1) Should it be the Fraud Team or DEWR.. Not previously mentioned 'DEWR FFT'.. Thoughts??

Commented ^S 22(1) : See last comment...

Commented ^S 22(1) First time referred to 'corruption'. Should this be mentioned further up the document? I think important to include BUT the FFT doesn't really address corruption.. Thoughts??

DEWR

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

FFT Partner agencies

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

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

Disclosure

Information collected and prepared for disclosure to the Taskforce and its Partners will be in accordance with appropriate legislation and clearance from the Information Legal Team (ILT). Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

DEWR intends to add restrictions to the release of information with the following wording:

The information is disclosed to the <INSERT DEPT> being a Commonwealth authority, as DEWR is satisfied it is necessary in order to enable or assist your agency/department to perform or exercise its powers or functions. Any further sharing of this information beyond the <INSERT DEPT> is to be approved by DEWR.

It is anticipated any release of information from DEWR to the Taskforce and its Partners will be either via DEWRs established CLAPOOM or PIC processes.

Release of information will most typically be in the form of an email from the FFT mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?	This will depend on the number of
---	-----------------------------------

	persons or entities flagged as concerning. (TBC)
--	--

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?	
If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.	Yes
☐ The <u>nature or type</u> of the personal information being handled is new or different.	
☐ The <u>scope</u> of the personal information being handled is new or different.	
☐ The personal information is being handled in a new or different <u>context</u> .	
☐ The <u>purpose</u> for which the personal information is being handled is new or different.	
☒ The <u>risk</u> of handling the personal information is new or different.	
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).	
You should provide the name of the same or similar project or initiative <u>where the practice(s) have been assessed previously</u> and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	
N/A	

Commented s 22(1) There is a new or changed way of handling personal information if any of the following apply:

- The handling relates to a completely new function or activity
- The department will be collecting more personal information than it used to or initiating a new collection
- The department will be using or disclosing the personal information for a different purpose than previously, including movement from paper based to electronic
- The department will be disclosing personal information to a third party that has not previously been disclosed
- A change is being made to how the personal information will be stored or disclosed
- A change is being made to who will have access to the personal information

Commented s 22(1) There needs to be more in common than just the means of handling (eg by email) for this to apply.

In addition, a privacy threshold assessment must have already been completed for the existing practice the handling is being compared to.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?	
To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	Choose an item.
☒ Handling large amounts of personal information.	
☒ Handling sensitive information ³ .	

Commented s 22(1) Whether a project or initiative is likely to have a significant impact on privacy depends on a range of factors.

The more of the factors below that apply the more likely the project or initiative is to have a significant impact on privacy. This includes if a security assessment has given the project or initiative a medium or high risk rating it should be considered as being likely to have a significant impact on privacy.

Commented s 22(1) This factor encompasses consideration of both the number of individuals whose personal information is being handled, the volume of personal information about those individuals, and the number of people internally and externally who have access to that personal information.

³ 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

☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
☐	Handling the personal information of individuals who are vulnerable. ⁴
☐	Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
☒	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☐	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.
☐	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☐	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
N/A	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
N/A	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	
N/A	

Commented s 22(1) This factor requires consideration of the potential consequences for the individual in the handling, and any potential mishandling, of their personal information. For example, if bank account details are involved there is the potential for financial loss from unauthorised access.

Commented s 22(1) This factor will apply if the project or initiative will be running for more than 3 months.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

Outcome	A PIA is required as there are or potentially are high privacy risk elements
---------	--

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: [Name/signature of Assistant Secretary or higher]

Date: Click or tap to enter a date.

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).

Document 16 (page 113-122) deleted under section 42(1) of the *Freedom of Information Act 1982* (Cth).

Document 17 (page 123-132) deleted under section 42(1) of the *Freedom of Information Act* 1982 (Cth).



Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code). This assessment should be completed after reading the PIA policy located [here](#).

Project or initiative

Brief project or initiative description and intended goals/outcomes

The PTA is an addendum to the previous Fraud Fusion Centre (FFC) – data sharing project's PTA and the approved PIA, signed 4 May 2024.

The addendum is to expand on the approach to the treatment and management of information sharing between the Department of Employment and Workplace Relations (DEWR), the Fraud Fusion Taskforce (Taskforce) and its Partners for Taskforce-approved operation/s (also known as Strikeforce/s) project/s or to partner agencies.

The Taskforce is jointly lead and operated by the National Disability Insurance Agency (NDIA) and Services Australia (SA) to prevent, detect and disrupt serious fraud. The Taskforce will enable intelligence sharing, identification and response by its Partners to identify and address fraud vulnerabilities and fraud-related activities perpetuated by Serious and Organised Crime (SOC) entities and others seeking to exploit the Government's programs.

Operation/s or project/s may be led by either the NDIA, SA or one of the Taskforce Partners. The lead will be determined on a case-by-case basis by the FFT Governance Framework – such as the FFT Operational Working Group, FFT Intelligence and Operations Committee or FFT Inter-Departmental Committee.

The lead Partner of these operation/s or project/s may determine to release, or request information from FFT partner agencies; the lead Partner will follow the Taskforces Memorandum of Understanding (MOU).

The MOU outlines the Taskforce purpose, its strategic focus, Governance and Responsibilities and how data, information sharing and security is to be handled by each Partner.

Clause 5 – Taskforce Purpose, paragraph 2 outlines the FFT’s:

- a) strategic focus on:
 - 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.**

Clause 5 – Taskforce Purpose, paragraph 4 outlines how the FFT:

- a) will 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 Clause 7 – Governance and Responsibilities - provides an overview of the agreed to operational conditions and management of the Taskforce. Clause 14 – Data, information sharing and security - provides the framework and management on how each Partner will manage the sharing of data and information, its security and disclosure.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Enterprise Risk, Assurance and Investigations Branch, Legal and Assurance Division, DEWR Compliance Intelligence, Skills Program Compliance Branch, Skills and Training Group, DEWR

	FEG Program Management Office, Entitlements Safeguards Division, Workplace Relations Group, DEWR Assurance Insights, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR Risk Management Insurance Incidents, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR Any and all relevant internal teams e.g., Skills Compliance Delivery, PALM etc. External Stakeholder/s: Any and all current and future FFT Partners.
--	---

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						Yes	
Type of information	Collect	Use	Disclose	Store	Destroy ²		
Names	☒	☒	☒	☒	☐	☐	
Signatures	☐	☐	☐	☒	☐	☐	
Addresses	☒	☒	☒	☒	☐	☐	
Email addresses	☒	☒	☒	☒	☐	☐	
Telephone numbers	☒	☒	☒	☒	☐	☐	
Dates of birth	☒	☒	☒	☒	☐	☐	
Sex or gender	☒	☒	☒	☒	☐	☐	
Opinions or feedback	☐	☐	☐	☐	☐	☐	
Commentary	☐	☒	☒	☒	☐	☐	
CRNs or JSIDs	☐	☒	☒	☒	☐	☐	
USIs or CHESSNs	☐	☒	☒	☒	☐	☐	

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☒	☒	☒	☒	☐	☐
Bank account details	☒	☒	☒	☒	☐	☐
Identity documents	☐	☒	☒	☒	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Partnership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Partnerships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☐	☐	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/A						
How will personal information be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative? <i>You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.</i>						
The DEWR FFT team will be the central point of contact for all requests and release of information. Information Sharing No information will be requested from individuals directly associated with DEWR programs, all information gathered will be via DEWR's already established data holdings e.g., ESS, ADMS, TYIMS, FEG, ESS Tip-off and iBase etc. Additional information may be sourced through paid third parties e.g., Equifax or open source such as ABN lookup or Google. The lead agency may initiate and facilitate information sharing, by:						

Public Interest Certificate (PIC) or CLAPOOM

- a) any release of information from the lead agency to DEWR will be the responsibility of the lead agency to ensure they met and adhered to any relevant legislation and data policy (of their department and FFT MOU) to release the information to the other FFT Partners.

The lead agency releasing information may request data from DEWR to enable the FFT meet its strategic purposes. The information requested will be but not limited to:

- Previous or current compliance or fraud activities against certain organisations or individuals,
- Contact details of individuals,
- Bank account details, etc.

Request for Information (RFI)

- b) the lead agency may request DEWR review its data holdings and provide specific information about companies, people and payments. The information requested will be but not limited to:
- Previous or current compliance or fraud activities against certain organisations or individuals,
 - Contact details of individuals,
 - Bank account details, etc.

DEWR Release of Information

DEWR's FFT team through an intelligence led process may release information, proactively or as per a RFI, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption. The lead agency may then release this information to other FFT Partners.

The nature of information collected and released may vary depending on the type of request, we believe the information will fall within these categories:

- (a) material that is both personal and protected information;
- (b) material that is personal but not protected information; and
- (c) material that is neither personal nor protected information (where the information has not been obtained under any law and relates to a business or person).

Storage

DEWR

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

FFT Partner agencies

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

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

Disclosure

Information collected and prepared for disclosure to the Taskforce and its Partners will be assessed by the FFT team to ensure any release be considered carefully and released in line with relevant legislation, personal information management requirements and previous legal advice received from the Information Legal Team (ILT). If required advice may be sort from the ILT to ensure our assessment to release or not is correct and accurate.

DEWR intends to add restrictions to the release of information with the following wording:

The information is disclosed to the <INSERT DEPT> being a Commonwealth authority, as DEWR is satisfied it is necessary to enable or assist your agency/department to perform or exercise its powers or functions. Any further sharing of this information beyond the <INSERT DEPT> is to be approved by DEWR.

It is anticipated any release of information from DEWR to the Taskforce and its Partners will be either via DEWRs established CLAPOOM or PIC processes.

Release of information will most typically be in the form of an email from the FFT mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce officers.	
How many individuals' personal or sensitive information will be handled in the project or initiative?	This will depend on the number of persons or entities flagged as concerning. (TBC)

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way? If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.	Yes
☐ The <u>nature or type</u> of the personal information being handled is new or different.	
☐ The <u>scope</u> of the personal information being handled is new or different.	
☐ The personal information is being handled in a new or different <u>context</u> .	
☐ The <u>purpose</u> for which the personal information is being handled is new or different.	
☒ The <u>risk</u> of handling the personal information is new or different.	
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s). You should provide the name of the same or similar project or initiative <u>where the practice(s) have been assessed previously</u> and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	
N/A	

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals? To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	Yes
☒ Handling large amounts of personal information.	

☒	Handling sensitive information ³ .
☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
☒	Handling the personal information of individuals who are vulnerable. ⁴
☒	Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
☒	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☐	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.
☒	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☐	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
N/A	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
N/A	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	
N/A	

³ 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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	A PIA is required as there are or potentially are high privacy risk elements
---------	--

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by ^{s 22(1)}

Date: 20/01/2025

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Threshold Assessment

Fraud Fusion Taskforce: Information sharing and data management between partner agencies.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code). This assessment should be completed after reading the PIA policy located [here](#).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The PTA is an addendum to the previous Fraud Fusion Centre (FFC) – data sharing project’s PTA and the approved PIA, signed 4 May 2024. The addendum is to expand on the approach to the treatment and management of information sharing between the Department of Employment and Workplace Relations (DEWR), the Fraud Fusion Taskforce (Taskforce) and its Partners for Taskforce-approved operation/s (also known as Strikeforce/s) project/s or to partner agencies. The Taskforce is jointly lead and operated by the National Disability Insurance Agency (NDIA) and Services Australia (SA) to prevent, detect and disrupt serious fraud. The Taskforce will enable intelligence sharing, identification and response by its Partners to identify and address fraud vulnerabilities and fraud-related activities perpetuated by Serious and Organised Crime (SOC) entities and others seeking to exploit the Government’s programs. Operation/s or project/s may be led by either the NDIA, SA or one of the Taskforce Partners. The lead will be determined on a case-by-case basis by the FFT Governance Framework – such as the FFT Operational Working Group, FFT Intelligence and Operations Committee or FFT Inter-Departmental Committee.
--	--

The lead Partner of these operation/s or project/s may determine to release, or request information from FFT partner agencies; the lead Partner will follow the Taskforces Memorandum of Understanding (MOU).

The MOU outlines the Taskforce purpose, its strategic focus, Governance and Responsibilities and how data, information sharing and security is to be handled by each Partner.

Clause 5 – Taskforce Purpose, paragraph 2 outlines the FFT’s:

- a) strategic focus on:
 - 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.**

Clause 5 – Taskforce Purpose, paragraph 4 outlines how the FFT:

- a) will 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 Clause 7 – Governance and Responsibilities - provides an overview of the agreed to operational conditions and management of the Taskforce. Clause 14 – Data, information sharing and security - provides the framework and management on how each Partner will manage the sharing of data and information, its security and disclosure.
Key implementation date/s	TBC
Key internal and external stakeholders	Internal Stakeholder/s: Fraud Intelligence and Investigations Team (Fraud Team), Enterprise Risk, Assurance and Investigations Branch, Legal and Assurance Division, DEWR Compliance Intelligence, Skills Program Compliance Branch, Skills and Training Group, DEWR

	FEG Program Management Office, Entitlements Safeguards Division, Workplace Relations Group, DEWR Assurance Insights, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR Risk Management Insurance Incidents, Quality Assurance and Risk Management Branch, Employment and Workforce Group, DEWR External Stakeholder/s: Any and all current and future FFT Partners.
--	--

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information ¹ ?						Yes	
- If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.							
Type of information	Collect	Use	Disclose	Store	Destroy ²	De-identify	
Names	☐	☒	☒	☐	☐	☐	
Signatures	☐	☒	☒	☐	☐	☐	
Addresses	☐	☒	☒	☐	☐	☐	
Email addresses	☐	☒	☒	☐	☐	☐	
Telephone numbers	☐	☒	☒	☐	☐	☐	
Dates of birth	☐	☒	☒	☐	☐	☐	
Sex or gender	☐	☒	☒	☐	☐	☐	
Opinions or feedback	☐	☒	☒	☐	☐	☐	
Commentary	☐	☒	☒	☐	☐	☐	
CRNs or JSIDs	☐	☒	☒	☐	☐	☐	
USIs or CHESSNs	☐	☒	☒	☐	☐	☐	
Tax file numbers	☐	☐	☐	☐	☐	☐	
Financial information	☐	☒	☒	☐	☐	☐	
Bank account details	☐	☒	☒	☐	☐	☐	

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.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Identity documents	☐	☒	☒	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Partnership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Partnerships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☒	☒	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/A						
How will personal information be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative? <i>You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.</i>						
The DEWR FFT team will be the central point of contact for all requests and release of information. Information Sharing No information will be requested from individuals directly associated with DEWR programs, all information gathered will be via DEWR's already established data holdings e.g., ESS, ADMS, TYIMS, FEG, ESS Tip-off and iBase etc. Additional information may be sourced through paid third parties e.g., Equifax or open source such as ABN lookup or Google. The lead agency may initiate and facilitate information sharing, by: <u>Public Interest Certificate (PIC) or CLAPOOM</u>						

- a) any release of information from the lead agency to DEWR will be the responsibility of the lead agency to ensure they met and adhered to any relevant legislation and data policy (of their department and FFT MOU) to release the information to the other FFT Partners.

The lead agency releasing information may request data from DEWR to enable the FFT meet its strategic purposes. The information requested will be but not limited to:

- Previous or current compliance or fraud activities against certain organisations or individuals,
- Contact details of individuals,
- Bank account details, etc.

Request for Information (RFI)

- b) the lead agency may request DEWR review its data holdings and provide specific information about companies, people and payments. The information requested will be but not limited to:

- Previous or current compliance or fraud activities against certain organisations or individuals,
- Contact details of individuals,
- Bank account details, etc.

DEWR Release of Information

DEWR's FFT team through an intelligence led process may release information, proactively or as per a RFI, if it believes the information will help facilitate a whole of Government approach to the detection, prevention, and treatment of serious or systemic fraud and corruption. The lead agency may then release this information to other FFT Partners.

The nature of information collected and released may vary depending on the type of request, we believe the information will fall within these categories:

- (a) material that is both personal and protected information;
- (b) material that is personal but not protected information; and
- (c) material that is neither personal nor protected information (where the information has not been obtained under any law and relates to a business or person).

Storage

DEWR

Information will be stored in the department's preferred records management system in line with its records management policy for example, O Drive and/or Content Manager, Fraud Fusion Taskforce mailbox, Sharepoint, TRIM and/or the department's web-based secure File Transfer system. Access to this information will be restricted to persons involved with the Fraud Team and will hold a Negative Vetting Level 1 clearance.

The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) with procedures being put in place by DEWR's database administrators (DBA). The DEWR server is located in Canberra, ACT.

FFT Partner agencies

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

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

Disclosure

Information collected and prepared for disclosure to the Taskforce and its Partners will be in accordance with appropriate legislation and clearance from the Information Legal Team (ILT). Each request will be considered carefully and released in line with relevant legislation and personal information management requirements.

DEWR intends to add restrictions to the release of information with the following wording:

The information is disclosed to the <INSERT DEPT> being a Commonwealth authority, as DEWR is satisfied it is necessary in order to enable or assist your agency/department to perform or exercise its powers or functions. Any further sharing of this information beyond the <INSERT DEPT> is to be approved by DEWR.

It is anticipated any release of information from DEWR to the Taskforce and its Partners will be either via DEWRs established CLAPOOM or PIC processes.

Release of information will most typically be in the form of an email from the FFT mailbox or by File Transfer, be classified 'Official: Sensitive' and be accessed by Taskforce officers.

How many individuals' personal or sensitive information will be handled in the project or initiative?

This will depend on the number of

	persons or entities flagged as concerning. (TBC)
--	--

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way? If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.	Yes
☐ The <u>nature or type</u> of the personal information being handled is new or different.	
☐ The <u>scope</u> of the personal information being handled is new or different.	
☐ The personal information is being handled in a new or different <u>context</u> .	
☐ The <u>purpose</u> for which the personal information is being handled is new or different.	
☒ The <u>risk</u> of handling the personal information is new or different.	
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s). You should provide the name of the same or similar project or initiative <u>where the practice(s) have been assessed previously</u> and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	
N/A	

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals? To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	Choose an item.
☒ Handling large amounts of personal information.	
☒ Handling sensitive information ³ .	

³ 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

☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
☐	Handling the personal information of individuals who are vulnerable. ⁴
☐	Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
☒	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☐	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.
☐	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☐	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
N/A	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
N/A	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	
N/A	

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

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.

⁴ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.

Outcome	A PIA is required as there are or potentially are high privacy risk elements
I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements. Approved by _____ s 22(1) Date: 28/01/2025 A copy of this privacy threshold assessment must be retained on file and sent to the Privacy Officer.	

Document 20 (page 153-174) deleted under section 42(1) of the *Freedom of Information Act 1982* (Cth).

Document 21 (page 175-185) deleted under section 42(1) of the *Freedom of Information Act 1982* (Cth).