

OFFICIAL: SENSITIVE

griffinlegal.



Australian Government
Department of Home Affairs

Department of Home Affairs
Open-source collection tools
Privacy Impact Assessment

FINAL
1 April 2025

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 47F(1)

Practical. Reliable. Quality.
Canberra | Melbourne
Partnering with Business,
Government, National Bodies,
Community Organisations & Sport.

CONTENTS

PART 1: EXECUTIVE SUMMARY	4
PART 2: RECOMMENDATIONS AND DEPARTMENT'S RESPONSE	5
PART 3: METHODOLOGY AND ASSUMPTIONS	8
PART 4: PROJECT DESCRIPTION	10
PART 5: PERSONAL INFORMATION ANALYSIS	22
PART 6: COMPLIANCE WITH THE APPS.....	35
PART 7: PRIVACY IMPACT ANALYSIS AND COMPLIANCE CHECK	45
PART 8: ASSESSMENT OF DEPARTMENT PRIVACY POLICY	48
ANNEXURE A: GLOSSARY	50

REFERENCE SCHEDULE

Name of Project	Open-source Collection Tools		
Name of Client	The Department of Home Affairs		
Date	1 April 2025	PIA version number	v.05 - FINAL
PIA s. 47F(1)	s. 47F(1) Griffin Legal	Contact details	s. 47F(1) s. 47F(1) @griffinlegal.com.au
Client project manager	s. 22(1)(a)(ii)	Contact details	s. 22(1)(a)(ii) @homeaffairs.gov.au

VERSION HISTORY

Version	Date	Summary of changes
v.01	2 August 2024	Initial PIA provided to the Department
v.02	11 September 2024	Revised PIA incorporating the Department's feedback dated 2 September 2024
v.03	12 December 2024	Revised PIA based on ILS feedback dated 10 October 2024 and included additional open source tools
v.04	25 February 2025	Revised PIA based on further feedback for this and additional tools addendum PIA
v.05	1 April 2025	FINAL PIA based on ILS feedback dated 25 March 2025

PART 1: EXECUTIVE SUMMARY

Overview

- 1.1 The Department of Home Affairs (the **Department**) is responsible for central coordination, strategy and policy leadership in relation to cyber and critical infrastructure resilience and security, immigration, border security and management, counter-terrorism, the protection of Australia's sovereignty and citizenship, and social cohesion.
- 1.2 The Department, including the Australian Border Force (the **ABF**), utilises a number of commercial open-source information platforms to support operational priorities, active operations and projects within the Department's functions and activities. This can include information accessed from social media or other online sources for research and intelligence purposes to support broader investigations, decision-making and integrity activities.
- 1.3 This Privacy Impact Assessment (**PIA**) has been prepared for the purpose of assessing the Department's (which includes the ABF's) Intelligence Capability's utilisation of various open-source collection tools (the **Project**).
- 1.4 It is our view that the privacy risks associated with the Project can be appropriately managed and mitigated in accordance with the recommendations in this PIA.
- 1.5 This PIA addresses:
 - (a) recommendations and practical measures to address privacy risks – see paragraph 2.1; and
 - (b) compliance with the Australian Privacy Principles (**APPs**) contained in Schedule 1 of the *Privacy Act 1988* (Cth) (**Privacy Act**) – see **Part 6 – Compliance with the APPs**.

PART 2: RECOMMENDATIONS AND DEPARTMENT'S RESPONSE

Summary of recommendations

- 2.1 This PIA makes **11 recommendations**, including practical analysis for how the Department can manage, mitigate, or remove privacy risks associated with the Project:

	Relevant APP	Recommendations	Department's response
1.	N/A	We recommend the Department implement appropriate privacy risk management tools (such as additional privacy impact assessments or an addendum to this PIA) to assess privacy impacts if there are any material changes to the collection or handling of personal information associated with the Project, once the details are known (paragraph 3.11).	
2.	APP 1	We recommend the Department update its Privacy Policy to explain how the Department collects personal information from online open sources, including with the assistance of software, and ensure all the primary collection purposes have been included in the Privacy Policy (paragraph 5.2).	
3.	APP 3	Most of these collection purposes require s. 47G(1)(a) and we recommend the Department assess on a case-by-case basis to consider whether it would be unreasonable or impracticable to collect information directly from individuals to avoid jeopardising the collection purposes (paragraph 5.21).	
4.	APP 6	We recommend that Departmental staff who are permitted to use or disclose personal information collected via open-source tools in connection with enforcement related activities are provided with the following guidelines with respect to record keeping requirements: (a) the date of the use or disclosure; (b) details of the personal information that was used or disclosed;	

OFFICIAL: SENSITIVE

Relevant APP		Recommendations	Department's response
		(c) the enforcement body conducting the enforcement related activity; (d) if the entity used the personal information, how the personal information was used by the entity; (e) if the entity disclosed the personal information, who it disclosed the personal information to (this may be the enforcement body or another entity); and (f) the basis for the entity's 'reasonable belief'. This will help the entity assure itself that this exception applies, and it may be a useful reference if the entity later needs to justify its reasonable belief. (paragraph 5.47).	
5.	APP 8	s. 47E(d)	
6.	APP 10	We recommend the Department satisfy itself that it has appropriate mechanisms (such as standard operating procedures and system controls) to ensure the personal information it holds is accurate, up-to-date and complete and the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (paragraph 5.64).	
7.	APP 11	We recommend the Department satisfy itself that it has appropriate security mechanisms to protect the personal and sensitive information it holds in relation to the Project. This could include:	

Relevant APP		Recommendations	Department's response
		(a) ICT security mechanisms such as: (i) encryption; (ii) audits and monitoring; and (iii) backup and recovery; (b) internal standard operating procedures; (c) an appropriate Data Breach Response Plan; and (d) destruction and de-identification processes. (paragraph 5.69 and 5.70).	
8.	APP 11	We recommend the Department obtain a Security Risk Assessment (SRA) relating to the Project and consider implementing any recommendations forming part of the SRA (paragraph 5.72).	
9.	APP 11	We recommend the Department retain the records associated with the Project per existing Departmental records management protocols and the Records Authorities that apply to the Department's core activities (paragraph 5.78).	
10.	N/A	We recommend the Department ensures its Data Breach Response Plan appropriately considers information handling associated with the Project, to ensure that privacy breaches are identified and mitigated in a timely manner (paragraph 7.10).	
11.	N/A	As a privacy-positive strategy, we recommend a post-implementation audit after the deployment of the Project to assess whether any changes need to be made to functionality or processes to better protect the data. The Department may decide a practical timeframe for the post-implementation audit considering other changing factors, such as policy updates (paragraph 7.19).	

PART 3: METHODOLOGY AND ASSUMPTIONS

Introduction

- 3.1 The Department is a Commonwealth agency and must comply with the Privacy Act, the APPs, and the *Australian Government Agencies – Governance) APP Code 2017 (APP Code)*.
- 3.2 Section 33D of the Privacy Act defines a PIA as a written assessment of an activity or function (or project) that identifies the impact the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.
- 3.3 Section 12 of the APP Code requires agencies to conduct a PIA for all “high privacy risk projects” and states that:
- “...a project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.”*
- 3.4 The Project involves collection of open-source data, utilising tools and software platforms of various commercial vendors. These methods have been utilised since 2017.
- 3.5 The Office of the Australian Information Commissioner (OAIC) has published the *Guide to undertaking privacy impact assessments (PIA Guide)*, which advises:
- “A PIA may be useful more than once during the project’s development and implementation. It should be revisited and updated when changes to the project are considered. If there are substantial changes to how personal information will be handled or changes to an existing project, it may be necessary to undertake another PIA.”*
- 3.6 This PIA follows guidance published by OAIC in the PIA Guide. Further assessment of potential privacy impacts should be considered if the project scope changes materially from that described in this PIA, or if new and substantial information becomes known.
- 3.7 In completing this PIA, we have:
- (a) considered how personal information flows through the Project;
 - (b) considered the Project’s compliance with the Privacy Act, including the APPs;
 - (c) analysed the possible impacts on the privacy of individuals; and
 - (d) identified and recommended options for avoiding, minimising or mitigating negative privacy impacts associated with the Project.

Assumptions and limitations

- 3.8 Griffin Legal has prepared this PIA in consultation with the Department.
- 3.9 We have relied on the Department for a description of the Project and have drafted our analysis and recommendations on the assumption that the information provided by the Department during the initial meeting of 15 May 2024 and in the documents listed in paragraph 3.13 accurately reflect the Project.
- 3.10 Griffin Legal has been engaged to undertake this PIA at the instruction of the Department and considered only the handling of personal information by the Department's Intelligence Capability (the **Intelligence Capability**) with respect to the Project.
- 3.11 If it is anticipated that there will be material changes to the collection or handling of personal information associated with this Project, we **recommend** the Department implement appropriate privacy risk management tools (such as additional privacy impact assessments or an addendum to this PIA) to assess privacy impacts of the changes, once the details are known (**Recommendation 1**).
- 3.12 Privacy risk management tools should also ensure that the Department maintains compliant with the Privacy Act as it may be amended from time to time.

Documents reviewed

- 3.13 In preparing this PIA, the following documents were considered:
- (a) publicly available information on the software platforms and tools from commercial vendors;
 - (b) the Department's Privacy Policy; and
 - (c) documents provided by the Department.

PART 4: PROJECT DESCRIPTION

- 4.1 In considering the privacy scope of the Project, it is important to understand the background to the Project.

Background – Current State

- 4.2 The Department's Intelligence Capability, containing the dispersed intelligence teams formerly within the Department's Intelligence Division, utilises several commercial open-source information platforms to support operational priorities, active operations and projects within the Department's functions and enforcement related activities.
- 4.3 The Intelligence Capability provides a unique contribution to national intelligence to protect Australian borders through its assessment and analysis function. It is charged with enabling intelligence-led operational and policy outcomes for the Department. It provides intelligence products and analysis capabilities to support the Secretary of the Department of Home Affairs and the Commissioner of the Australian Border Force in their responsibilities to protect Australia's security, prosperity and cohesion.
- 4.4 In fulfilling its functions, the Intelligence Capability must consider the full legislative frameworks that provide the authority to produce this intelligence. The Intelligence Capability's activities are governed by several Acts, including the *Customs Act 1901* (Cth), the *Migration Act 1958* (Cth), *Australian Citizenship Act 2007* (Cth) and the *Australian Border Force Act 2015* (Cth).
- 4.5 Accessing online and open-source information must be necessary for a specific function, proportionate to the objective in question and in accordance with the law and are listed as follows:

Privacy Act	The Privacy Act outlines considerations when collecting personal and sensitive information in APP 3 (contained in Schedule 1 to the Privacy Act). The collection of personal information is only permitted when the information is reasonably necessary for, or directly related to the Department's functions or activities, and must only be collected by lawful and fair means. The Department must not collect 'sensitive information' about an individual without the consent of that individual (and where this collection is also reasonably necessary for or directly related to the Department's functions or activities), unless an exception applies. Exceptions in the Privacy Act that allow the Department to lawfully collect sensitive information include: • when the collection is required or authorised by another law; or, • where the Department reasonably believes that the collection is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of the Department.
--------------------	---

	The Privacy Act defines the term 'enforcement related activities' to include, amongst other things, the conduct of surveillance, intelligence gathering or monitoring activities. While collection of sensitive information about an individual generally requires consent, there are situations where consent is not required if a 'permitted general situation' exists (APP 3.4(b)). This exception applies in relation to the collection of sensitive information (APP 3.4) and the use or disclosure of personal information (APPs 6.2 and 8.2). The APP entity is nevertheless required to comply with the rest of the APP requirements such as keeping information secure (APP 11) even though consent is not required. There are five relevant permitted general situations listed in s 16A of the Privacy Act (s 16A exception activities): • lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety (see APPs 3.4(b), 6.2(c) and 8.2(d)) • taking appropriate action in relation to suspected unlawful activity or serious misconduct (see APPs 3.4(b), 6.2(c) and 8.2(d)) • locating a person reported as missing (see APPs 3.4(c), 6.2(c) and 8.2(d)) • asserting a legal or equitable claim (see APPs 3.4(c) and 6.2(c)) • conducting an alternative dispute resolution process (see APPs 3.4(b) and 6.2(c)) The Department may rely on these exceptions when Open Source Collection Tools are being used for one of the purposes listed under S16A of the Privacy Act. The Tools are generally used for investigations and intelligence gathering. From the list of exceptions, it may be most relevant to the Department if the Department needs to use these tools to prevent a threat to public safety or to take appropriate action in relation to suspected unlawful activity or serious misconduct.
Migration Act 1958 (Cth) (the Migration Act)	The Migration Act outlines functions and activities of the Department, and provides both specific and implied authority for the Department to conduct information collection. The Department is subject to Migration Act restrictions relating to the handling of 'identifying information', which is defined in section 336A of the Migration Act, unless permitted under Part 4A of the Migration Act. Investigating an offence against a law of the Commonwealth or a State or Territory is not a

	permitted purpose under Part 4A of the Migration Act (section 336D(3)(a) and 336E(3)).
Australian Border Force Act 2015 (Cth) (the ABF Act)	Part 6 of the ABF Act prohibits the making of a record or disclosure of Immigration and Border Protection Information (IBP Information), subject to certain exceptions. Part 6 of the ABF Act provides that entrusted persons can only make a record of or disclose IBP information when certain exceptions apply, such as where disclosure is authorised by a provision of Part 6 of the ABF Act. For example, entrusted persons authorised by the Secretary under section 44(3) of the ABF Act can disclose IBP Information which contains personal information collected from open source tools under s 44(2) to a body or person mentioned in section 44(4) provided that the Secretary (or their delegate) is satisfied that it is necessary for a purpose mentioned in section 46 (see paragraph 4.6 below) and that the IBP information will enable or assist that body or person to perform or exercise any of the functions, duties or powers of that body or person; and provided that any conditions imposed under section 44(6) are satisfied. Under section 42(2)(b) of the ABF Act, the making of the record or disclosure of IBP Information by an entrusted person is not an offence if the disclosure is during the course of the person's employment or service as an entrusted person.
Customs Act 1901 (Cth) (the Customs Act)	The Customs Act outlines functions and activities of the Department, and provides both specific and implied authority for the Department to conduct information collection.
Australian Citizenship Act 2007 (Cth) (the Citizenship Act)	The Citizenship Act outlines functions and activities of the Department, and provides specific and implied authority for the Department to conduct information collection.

4.6 The permitted purposes set out in section 46 of the ABF Act, which are relevant to disclosures of IBP Information which contain personal information under s 44(2) and 45(2) of the ABF Act and are potentially relevant to this PIA are:

- (a) the administration or enforcement of Australian and foreign criminal laws, laws that impose pecuniary penalties or laws that involve the forfeiture of property;
- (b) in relation to the above laws, the prevention of crime or the detection or analysis of criminal conduct in respect of those laws;
- (c) assisting a coronial inquiry, investigation or inquest under Commonwealth, State or Territory law;
- (d) a purpose relating to the protection of public health or the prevention or elimination of risks to the life or safety of an individual or group of individuals;
- (e) the protection of the public revenue of the Commonwealth, a State, a Territory or a foreign country;

- (f) the establishment of a person's identity, citizenship status or visa status at any given moment in time;
 - (g) a purpose relating to immigration, quarantine or border control between Australia and a foreign country;
 - (h) the performance of functions under:
 - (i) section 17 of the *Australian Security Intelligence Organisation Act 1979*;
 - (ii) section 6 of the *Intelligence Services Act 2001*;
 - (iii) section 7 of the *Office of National Intelligence Act 2018*;
 - (i) the inter-country adoption of a child;
 - (j) the protection of national security or the defence of Australia;
 - (k) locating a missing person; or
 - (l) a purpose prescribed by the rules.
- 4.7 Section 6(1) of the *Privacy Act* includes the Immigration Department, which functions and responsibilities have been subsumed by the Department of Home Affairs, as an 'enforcement body'.
- 4.8 Section 6(1) of the *Privacy Act* defines an 'enforcement related activity' as:
- (a) the prevention, detection, investigation, prosecution or punishment of:
 - (i) criminal offences; or
 - (ii) breaches of a law imposing a penalty or sanction; or
 - (b) the conduct of surveillance activities, intelligence gathering activities or monitoring activities; or
 - (c) the conduct of protective or custodial activities; or
 - (d) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (e) the protection of the public revenue; or
 - (f) the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations; or
 - (g) the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.
- 4.9 The Department's enforcement related activities include activities relating to both customs and immigration, such as:
- (a) detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law;
 - (b) identifying and locating unlawful non-citizens and resolving their immigration status, including the removal of unlawful non-citizens from Australia;
 - (c) preventing and reducing irregular migration, people smuggling and trafficking in persons;
 - (d) identifying and assessing claims by non-citizens for protection in Australia, including managing the detention or release into the community of protection claimants;
 - (e) assessing and enforcing compliance with visa and citizenship requirements;

- (f) identifying and assessing prior to arrival those entitled to lawfully enter Australia;
- (g) managing the entry and departure of people crossing the Australian border;
- (h) resolving the identity, health, national security and criminal history status of people applying to enter Australia;
- (i) collecting and assessing information to assess the identity, character and criminal history of applicants for Australian citizenship; and
- (j) cooperation with other agencies, including information-sharing, for law enforcement and border security purposes, and the protection of the public revenue; and
- (k) Enforcement activities under the *Customs Act 1901*.

Open Source Tools

Maltego

- 4.10 We understand that the Department utilises the enterprise version of Maltego in support of their open-source intelligence (**OSINT**) capabilities. Specifically, the Department uses this tool, exclusively within the Online and Geospatial Intelligence Section (**OGI**), in line with its open-source collection policy, where it is reasonably necessary for a Departmental function.
- 4.11 Maltego is a link analysis software which provides real-time data mining and information gathering, as well as the representation of this information on a node-based graph, outlining patterns and multiple order connections between information. The outputs provided by the Maltego software allows for the identification of crucial links, identifies presence across data sources, and the uncovering of intelligence insights.

Functional capabilities

- 4.12 Maltego software analyses real-world relationships between information that is publicly accessible on the Internet. Maltego can be used to gather information on the Internet infrastructure underlying a domain, including the related subdomains, Internet Protocol (**IP**) addresses, email addresses, and the relationship between that domain and other entities (also known as network foot-printing).
- 4.13 Maltego can also be used to query sources such as Domain Name System (**DNS**) records, WHOIS records, search engines, social networks, various online Application Programming Interfaces (**APIs**) and extracting meta data to determine the relationships between:¹
- (a) individuals, as represented by their names, email addresses or aliases;
 - (b) groups of individuals (social networks);
 - (c) companies;
 - (d) organisations;
 - (e) websites;
 - (f) Internet infrastructure, including domains, DNS records, Netblocks, IP addresses;
 - (g) affiliations; and

¹ Maltego, 'What can I use Maltego for?', Maltego (Webpage, 8 May 2024)
<<https://docs.maltego.com/support/solutions/articles/15000020188-what-can-i-use-maltego-for->>.

(h) documents and files.

- 4.14 Maltego integrates with external data sources, including OSINT platforms, internal databases, and proprietary APIs. The data integration capabilities support traditional sources and emerging technologies including blockchain and Internet of Things (IoT) devices.
- 4.15 Maltego ensures users stay up-to-date with the latest data sources by integrating new data feeds and APIs adaptively.

Babel Street Insights

- 4.16 We understand that the Department utilises Babel Street Insights in support of their OSINT capabilities. This software is currently only used within OGI.
- 4.17 Babel Street Insights is a multilingual, geo-enabled analytics platform which assists with threat intelligence, identity resolution, and risk mitigation.

Functional capabilities

S. 47(1)(a)

Locate X

- 4.19 The Department utilises Locate X in support of their OSINT capabilities.
- 4.20 Locate X is a software that enables users to draw a digital fence around a defined geographic area, identifies the location of mobile devices s. 47G(1)(a) Mobile devices are only identified

through anonymised advertising ID's, and not unique identifiers for the physical handsets.

Functional capabilities

4.21 Locate X uses s. 47G(1)(a)

s. 47G(1)(a)

4.22 Locate X uses s. 47G(1)(a)

s. 47G(1)(a)

4.23 The availability of some Locate X Data may be limited in accordance with various national privacy and/or data protection laws, including the GDPR. Where a customer can certify its exemption to the GDPR, additional Locate X data may be available.

Sprinklr

4.24 The Department utilises Sprinklr OIS in support of their OSINT capabilities. The Department's Intelligence Capability uses Sprinklr on a limited basis, for monitoring purposes to achieve its intelligence and operational functions and activities.

4.25 Sprinkler OIS operates as a cloud-based Software as a Service (**SaaS**) with all Australian customers accessing the same version of the Platform via the Internet. Sprinklr OIS is hosted in a Virtual Private Cloud (**VPC**) within a multi-tenant hosted environment, logically isolated from other Sprinklr customer instances that share the same physical servers.

Functional capabilities

4.26 Sprinklr OIS was developed as a unified customer experience management platform for social engagement and front office management, which encompasses several products and services. Sprinklr OIS is used by the Department to provide the following functions:

- (a) social listening, which involves the identification and assessment of information or opinions of an entity on the Internet;
- (b) management of user accounts with access to social channels; and
- (c) publication of information by those users on social channels.

- 4.27 Sprinklr OIS' platform enables integration with multiple digital channels for users, including Customer Relationship Management (**CRM**) systems, public media sources such as social media posts, reviews, blog posts, and social media account metadata. This enables the unilateral assessment on the scope, source, and type of data being processed.
- 4.28 Sprinklr OIS also uses Artificial Intelligence (**AI**) to create insights and provide deeper, real-time user experiences.
- 4.29 The Sprinklr IOS platform enables users to connect, engage and service their own customers, including through the processing of publicly accessible online information. Sprinklr also provides enablement, success management, transformation, analytics and moderation services for customers.

ShadowDragon SocialNet

- 4.30 The Department utilises the ShadowDragon SocialNet (**ShadowDragon**) for online investigations on individuals being investigated on account of being suspected of criminal activity (target entity) by analysts within OGI, in pursuit of investigative functions, where permitted under the open source policy.
- 4.31 ShadowDragon is an open source social media s. 47G(1)(a) and investigations software application developed by ShadowDragon, a company based in the United States. ShadowDragon operates under a SaaS licensing model, which allows the Department to access the software on external servers on a subscription basis rather than deploying it on existing Department infrastructure. ShadowDragon connects to the Department's platform and facilitates online investigations on individuals suspected of criminal activity (target entity) by analysts within the Department. All information collected and used by ShadowDragon is data that is publicly available on online social networks and does not include private messages.

Functional capabilities

- 4.32 ShadowDragon facilitates the collection and analysis of open source intelligence by:
- (a) enabling real-time queries of data publicly available on the Internet from over 150 social networks, including social media platforms, gaming discussion forums, online product reviews, or other forums and websites that offer illicit goods and/or services;
 - (b) mapping online connections to more accurately resolve online identities with the real-world entities they represent, and improve queries of networks and user cohorts;
 - (c) identifying social media associates of target entities to widen the scope of investigations;
 - (d) data analytics to enable discovery and visualisation of a target entity's social network, and cross-reference the data to establish correlations between actors to chart large and complex criminal operations;
 - (e) discover locations of assets or individuals and infer geographical attribution to create a map of suspicious activity and/or track target entities; and
 - (f) use the artifacts discovered to uncover lost assets and enable asset tracking.

- 4.33 ShadowDragon does not enable developer-level access to social media platforms or circumvent any encryption or privacy settings set up by individuals within the online platform/service hosting their data. It was designed and built to prevent its use for:
- discovery of private data that is otherwise inaccessible by members of the public; or
 - the collection and analysis of information of everyone, as opposed to restricting the collection of information to specific entities under suspicion (also known as dragnet surveillance).

Authentic8 Silo + ToolboxDW

- 4.34 The Department utilises Silo and ToolboxDW in support of their OSINT capabilities.
- 4.35 Silo is a secure and isolated cloud browser designed for anonymised access to the Internet, limiting the exposure of an analyst's digital fingerprint as they conduct investigations across the surface, deep, and dark web.
- 4.36 ToolboxDW offers the managed attribution feature in Silo, which creates separate virtual browser instances distributed across various geographic locations, along with platform and location spoofing capabilities so that researchers and investigators can quarantine the risks of accessing the Dark Web by doing so at an arms-length.
- 4.37 We understand Silo has the following use cases:

Area	Use Case
Digital investigations and intelligence	- Cybersecurity intelligence - Trust and safety - Intelligence and evidence gathering - Fraud and brand misuse - Financial crime and compliance - Corporate research and protection
Enhancing SASE capabilities	- Third-party application access - Bring Your Own Device (BYOD) application access - Secure application workspace
Eliminate web browsing risks	- Untrusted website access - Personal browsing - Enterprise browser

Functional capabilities - Silo

- 4.38 Silo is a cloud-based secure web browser application, which creates an insulation layer between the computer and the web service being accessed. Silo enables the management of login credentials, access controls and data use policies.

- 4.39 Silo consists of two products, Silo Web Isolation Platform and Silo for Research. We understand the Department is primarily using the Silo Web Isolation Platform² service, which includes:
- (a) a secure cloud-native execution environment solution for all web-based activity;³
 - (b) built on the principles that all web code and critical data should be isolated from the endpoint, and that browsing capabilities should be configurable and auditable;
 - (c) seamless deployment - Silo can be delivered as a distinct browser or seamlessly integrated into the existing browser using API;
 - (d) role based provisioning - Lets users define access, authentication and use policies across users and organisations; and
 - (e) integrates with IT services – Silo can interact seamlessly with current IT technology stacks, or act in a standalone environment and execute outside your organisation's infrastructure.
- 4.40 A small number of Silo for Research accounts exist within the Department. The Department uses Silo for Research to select a VPN exit node, allowing the Department's intelligence analysts to select from what location their internet browsing appears from appropriate to the research being undertaken.

Functional capabilities – ToolboxDW

4.41

s. 47G(1)(a)

- 4.42 ToolboxDW is an advanced version of Toolbox with Dark Web capabilities. This product option extends the reach of Silo+Toolbox into the Dark Web, delivering separate, geographically distributed virtual browser instances with platform and location spoofing functions. Users may interact with web-based content, including Dark Web, through their local host, but choose an alternative egress location, platform and language.
- 4.43 In order to access the Dark Web, usually a usability penalty is involved, and browsers need to be equipped with specific software, or network infrastructure needs specific configuration changes in order to access dark web resources. The underlying encryption routines associated with traffic over the dark web is called 'onion routing' and places an additional performance tax on the accessor. Even once configured, 'onion-capable' browsing solutions still terminate HTTP connections to the organisation's network and deliver the page payload to the local device for rendering, which exposes the organisation to malicious content. Toolbox DW is supposed to function as a simple, integrated workflow to interact with '.onion' content with intuitive data capture capabilities whilst keeping content in an isolated host.⁴

s. 47G(1)(a)

² Authentic8, 'Silo Web Isolation Platform', Authentic8 (Webpage, 2024) <<https://www.authentic8.com/products/silo-web-isolation-platform>>.

³ Authentic8, *Silo Web Isolation Platform – Data Sheet* (2024) <https://www.authentic8.com/sites/default/files/content/PDF_files/ds-silo-web-isolation-platform.pdf>.

⁴ Page 18 of ADD2017 1538111 Signed C4231807 Authentic8 Silo + Toolbox + DW SP

s. 47G(1)(a)

Web-IQ Voyager

4.45 Web-IQ Voyager is a software platform designed for digital investigations and online intelligence gathering. The Department's Intelligence Capability currently utilises this software in line with its open source collection policy, where it is reasonably necessary for a Departmental function.

Functional capabilities

4.46 Web-IQ Voyager has the following capabilities:

- (a) **Web Monitoring:** It allows users to monitor various online platforms such as social media, forums, and websites in real-time.
- (b) **Data Collection:** The software collects and aggregates data from different sources on the internet, including open web sources and social media APIs.
- (c) **Analysis Tools:** It provides tools for analysing collected data, such as sentiment analysis, network analysis, and keyword search functionalities.

s. 47(1)(a)

- (e) **Report Generation:** It enables the creation of comprehensive reports based on the analysed data, which can be used for legal proceedings or internal decision-making.
- (f) **Customization:** Depending on the version and customization options, Web-IQ Voyager may offer additional features tailored to specific investigative needs, such as geolocation tracking, image recognition, or integration with other investigative tools.

Web-IQ DarkCloud

4.47 Web-IQ DarkCloud is a specialised software platform designed for analysing the Dark Web, Telegram, Discord and chat boards. The Department's Intelligence Capability currently utilises this software in line with its open source collection policy, where it is reasonably necessary for a Departmental function.

Functional capabilities

s. 47(1)(a)

- (b) Threat Intelligence: It provides real-time threat intelligence by tracking discussions, transactions, and behaviour associated with cybercrime, terrorism, and other illicit activities.
- (c) Automated Monitoring: DarkCloud uses automated tools to continuously scan the dark web for keywords, patterns, and indicators of criminal behaviour, helping to identify emerging threats.
- (d) Data Aggregation: It collects and aggregates data from various dark web sources, allowing investigators to analyse trends, networks, and potential threats.
- (e) Visualization Tools: The platform often includes visualization tools to map out connections between different actors, organizations, and activities within the dark web ecosystem.
- (f) Alerting and Reporting: DarkCloud generates alerts and reports based on its findings, enabling proactive responses to threats and supporting legal actions or operational decisions.
- (g) Customizable Filters and Queries: Users can customize filters and queries to tailor the monitoring and analysis to specific threats or investigative priorities.

Benefits of the Project

- 4.49 The Project will assist the Department to research publicly available data to assist with investigations and several enforcement related activities in order to respond to threats.

PART 5: PERSONAL INFORMATION ANALYSIS

Privacy Policy

- 5.1 The declared object of APP 1 is 'to ensure that APP entities manage personal information in an open and transparent way'. This enhances the accountability of APP entities for their personal information handling practices and can build community trust and confidence in those practices.
- 5.2 The Department's Privacy Policy identifies that personal information may be collected from other sources, such as publicly available sources. However, the Privacy Policy does not specifically call out the methods by which the Department utilises to collect personal information from publicly available sources. While APP 1.4(b) states that the usual approach to collecting personal information must be explained in the Privacy Policy, to strengthen compliance with APP 1, in furtherance of accountability and transparency, we **recommend** the Department include how personal information is collected from online open sources, including with the assistance of software, and ensure all the primary collection purposes have been included in the Privacy Policy (**Recommendation 2**).
- 5.3 The Department's Privacy Policy expressly identifies that the Department is an enforcement body for the purposes of the *Privacy Act* and as such, can collect, use and disclose personal and sensitive information where it is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by or on behalf of the Department, or another enforcement body.

Collection of personal information

- 5.4 In accordance with APP 3.1, the Department may only collect personal information about an individual where reasonably necessary for, or directly related to, one or more of the Department's functions and activities.
- 5.5 The Department's functions are conferred either by legislation or an executive scheme or arrangement established by government. The legislation which governs the use of Open Source Collection Tools by the Department are listed in paragraph 4.5.
- 5.6 'Reasonably necessary' in APP 3.1 requires that the collection of personal information by the Department be appropriate and adapted to the Department's functions and activities and not merely 'helpful' or 'desirable'.⁶ We understand that guidance is provided to the Department regarding how to determine whether collection of personal information will be reasonably necessary for the Department's functions and activities, including asking the following questions:
- (a) what is the value of the information to the particular activity being undertaken?
 - (b) has the use of such information been of assistance in similar circumstances in the past?
 - (c) can the information be obtained from an alternative source?
 - (d) what is the strength of the suspicion that has led the Department to want to obtain the information?

⁶ *Mulholland v Australian Electoral Commissioner* [2004] HCA 41 [39] (Gleeson CJ).

- 5.7 The Department utilises open-source information platforms to support operational priorities, active operations and projects within the Department's functions and activities for the following purposes: border management, visa compliance and immigration status resolution, certain Australian laws including criminal and community protection, and enforcement related activities such as detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law.
- 5.8 The Department has mentioned in its [Privacy Policy](#) Section 4 that it may collect personal information for the following purposes: border management, visa compliance and immigration status resolution, certain Australian laws including criminal and community protection, and enforcement related activities such as detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law.
- 5.9 We find the Department's collection of personal information necessary and directly related to the Department's functions as outlined in the Department's Privacy Policy and the Department's Online Open Source and Social Media Access Policy.
- 5.10 We note from the privacy policies of the Open Source Collection Tools that these tools may be collecting and using personal information for purposes not listed in their Privacy Policies and often the personal information collected by Open Source Collection Tools may be excessive and broad. We note this is beyond the Department's control to maintain or update privacy policies used by the Open Source Collection Tools. As our recommendations in this PIA are addressed to the Department, not to the Open Source Collection Tools, no recommendations can be made to the Department to address this issue.
- 5.11 APP 3.5 provides an APP entity must collect personal information 'only by lawful and fair means', which is an important safeguard to ensure that personal information can only be collected by lawful and fair means. In this particular project, Open Source Collection Tools generally collect public information available on the public internet from various sources. The standard of what is 'fair' presents an open-textured and evaluative criterion against which collection by an entity is to be assessed. Although the term 'fair' is not defined in the Privacy Act, in relation to the conception of fairness embodied in APP 3.5, the explanatory memorandum states that the OAIC has interpreted "fair" to mean "without intimidation or deception" or without use of means that are "unreasonably intrusive". When undertaking the assessment of whether a collection is 'fair' for the purposes of APP 3.5, all the circumstances must be considered. See 63F [49] of *Commissioner Initiated Investigation into Master Wealth Control Pty Ltd t/a DG Institute (Privacy)* [2024] AICmr 243.
- 5.12 In the *Master Wealth* case, the companies were found to have failed to collect the personal information by fair means, take reasonable steps to notify individuals whose information was collected, and to ensure that the information it collected was accurate and up to date. The companies collected personal information from court lists and databases for inclusion in their weekly leads lists, and whose personal information they subsequently disclosed to participants through those leads lists. We note that while this case provides references to how OAIC may interpret what lawful and fair means, 'lawful and fair' is not limited to collection with individual's knowledge. Whilst the sources of information collected by the Open Source Collection Tools are often not verified, the Department is collecting information "without intimidation or deception" and without use of means that are "unreasonably intrusive".
- 5.13 We also note that Open Source Collection Tools often use data scraping techniques to extract publicly available information from online sources. The **OAIC** and 11 other

international data protection and privacy authorities have previously released a joint statement, [Global expectations of social media platforms and other sites to safeguard unlawful data scraping](#) (**Statement**) to identify privacy risks involved in data scraping processes.

- 5.14 We have provided **Recommendation 2** to the Department to use the Department's Privacy Policy as a reasonable way to notify individuals about the Department's use of Open Source Collection Tools, include how personal information is collected via open-source collection tools and ensure all the primary collection purposes have been included in the Privacy Policy. The OAIC also included in the Statement that organisations can further protect users' information and reinforce user trust by actively informing their users of the steps they can take to protect their personal information. The Department should be mindful of the practices used by relevant Open Source Collection Tools and avoid using tools which collect information that is sourced from unlawful and unfair means for the purpose of this Project.
- 5.15 We **recommend** the Department review how personal information is collected by each Open Source Collection Tool, and satisfy itself that information is collected by lawful and fair means without intimidation, deception or use of means that are unreasonably intrusive (**Recommendation 2**).
- 5.16 APP 3.6 provides that an APP entity 'must collect personal information about an individual only from the individual' unless the individual consents to the collection of the information from someone other than the individual or it is unreasonable or impracticable for the entity to collect personal information only from the individual.
- 5.17 In this particular project, Open Source Collection Tools generally collect public information available on the internet. For example, individuals may not be aware that they have provided a broad consent to online social media sites, and they may not be aware that personal information publicly available on social media sites is collected by Open Source Collection Tools and used by customers of Open Source Collection Tools, like the Department, to conduct investigations and other purposes. We have also noted above Open Source Collection Tools often do not disclose in their Privacy Policies or Privacy Notices which platforms they collect personal information from, and whether they have obtained consent to collect such information. It is likely that some information collected by the Open Source Collection Tools is not directly collected from the individual nor with the individual's consent.
- 5.18 The *Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, page 77 provides examples of when it may be unreasonable or impracticable to collect personal information only from the individual concerned, for example, a law enforcement agency may be investigating an individual for a criminal offence, but that investigation could be prejudiced by the agency being forced to seek particular information directly from the individual. This exception allows long-standing type of activity to continue without breaching APP 3, and the exception is not limited to enforcement related activities.
- 5.19 The Department may be able to rely on the exception provided in APP 3.6(b) to avoid collecting information from the individual because it is "unreasonable or impracticable to do so". When the Department collects information for purposes of s 16A exception activities and enforcement related activities, it is unreasonable or impracticable to collect personal information only from the individual concerned, where the collection may not be practical or may jeopardise the investigation if the personal information is collected only from that individual (APP Guidelines 3.65). This scenario also fits the example provided in the *Explanatory Memorandum*.

- 5.20 When the Department collects information for purposes other than s 16A exception activities and enforcement related activities, if it is for an investigation, the Department can still rely on APP 3.6(b) exception and the example scenario provided in the *Explanatory Memorandum*.
- 5.21 If the Department collects information for purposes other than s 16A exception activities and enforcement related activities, the Department collects, uses and discloses personal information for the primary purposes of border management, community protections, investigations, intelligence and enforcement activities listed in paragraph 4.9 such as investigations and assessment. Most of these collection purposes require s. 47G(1)(a) and we **recommend** the Department assess on a case-by-case basis to consider whether it would be unreasonable or impracticable to collect information directly from individuals to avoid jeopardising the collection purposes (**Recommendation 3**).

Collection of sensitive information

- 5.22 The Department may only collect sensitive information about an individual with consent and where the information is reasonably necessary for the Department's functions or activities, or if an exception under APP 3.4 applies.
- 5.23 APP 3.4 provides that an APP entity can collect sensitive information without a person's consent, if the APP entity is an enforcement body and the entity reasonably believes that the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the enforcement body.
- 5.24 The requirement for there to be a 'reasonable belief' means that an objective assessment needs to be made in relation to whether the collection of the information by the Department is 'reasonably necessary for' the particular enforcement related activities, listed in paragraph 4.9, to be undertaken by the Department.
- 5.25 As an enforcement body, the Department may collect sensitive information where there is a reasonable belief that collecting the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the Department (APP 3.4(d)(i)).
- 5.26 APP 3.4(b) also provides seven permitted general situations in relation to the collection of sensitive information by the APP entity. We have included our analysis in paragraph 4.5 that the Department may rely on these exceptions when Open Source Collection Tools are being used for any of the s 16A exception activities.
- 5.27 For of this Project, the Department can only collect sensitive information if:
- (a) the Department has obtained an individual's consent, or
 - (b) it is for enforcement related activities purpose, or
 - (c) it falls within the list of s 16A exception activities.

Unsolicited personal information

- 5.28 APP 4 outlines the steps the Department must take if it receives unsolicited personal information. Unsolicited personal information is personal information received by the Department that has not been requested by the Department.
- 5.29 We understand that while search requests within the tools can provide search results that may include personal information, including sensitive information, that is not necessary for the functions of the Department, only the information that is relevant to an investigation is collected by Departmental Staff. No unsolicited personal information is expected to be collected for this Project.

Notification of the collection of personal information

- 5.30 APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.
- 5.31 The OAIC APP Guidelines provide that APP 5.1 acknowledges that it may be reasonable for an APP entity to not take any steps to provide a notice or ensure awareness of all or some of the APP 5 matters. It is the responsibility of the entity to be able to justify not taking any steps. One of the examples of when this may be reasonable is when Notification may jeopardise the purpose of collection or the integrity of the personal information collected and there is a clear public interest in the purpose of collection, for example, a law enforcement agency undertaking lawful covert surveillance of an individual in connection with a criminal investigation (OAIC APP Guidelines Chapter 5 APP 5 Notification of the collection of personal information paragraph 5.7).
- 5.32 In this Project, notification to individuals will jeopardise the purpose of the collection, for example, when the Department conducts an investigation on a person of interest. Therefore, it is not required for the Department to take reasonable steps outlined in APP 5.2 to notify individuals when conducting activities for a purpose that may be jeopardised by the notification.

Use and disclosure of personal information

- 5.33 Under APP 6, the Department may only use or disclose personal information about an individual for the purpose it was collected (**primary purpose**) or for another purpose (**secondary purpose**) with the individual's consent or where an exception in APP 6.2 applies.
- 5.34 The Department has mentioned in its [Privacy Policy](#) Section 4 that it may collect, use and disclose personal information for the following purposes: border management, visa compliance and immigration status resolution, certain Australian laws including criminal and community protection, and enforcement related activities such as detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law.
- 5.35 In this Project, the Department collects, uses and discloses personal information for the primary purposes of border management, community protections, investigations, intelligence and enforcement activities listed in paragraph 4.9 such as investigations and

assessment. The specific purpose applicable to a particular use of a Tool depends on the circumstances. The Department's primary use of personal information is aligned with the collection purposes outlined in its privacy policy.

- 5.36 The Department may also use personal information for secondary purposes beyond the original collection purpose, such as for research and reporting purposes.
- 5.37 If the Department uses Open Source Collection Tools for purposes beyond the primary purposes and relies on APP 6.2 as an exception, the Department needs to be mindful that for any use and disclosure purposes beyond the primary purposes, the secondary use and disclosure purpose must fall within one of the exceptions outlined in the APP 6.2:
- (a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose, and the secondary purpose is directly related the primary purpose (if the information is sensitive information), or related to the primary purpose (if the information is personal information);
 - (b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order;
 - (c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity;
 - (d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity;
 - (e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
- 5.38 In this Project, APP 6.2(b) may apply when the Department operates under a court order or where it is otherwise authorised or required by law. APP 6.2 (c) may apply if the use or disclosure of the information falls within one of the s 16A permitted general situations. APP 6.2(e) applies when the Department conducts enforcement related activities.
- 5.39 The Department may use or disclose personal information collected through the open source tools for a secondary purpose where, amongst others, the use or disclosure of the personal information is reasonably necessary for an enforcement related activity of the Department or if the Department considers that the use or disclosure of the information is necessary to prevent a serious threat to the life, health or safety of an individual or reasonably necessary to assist in locating a person who has been reported as missing. These disclosures remain compliant with APP 6.
- 5.40 The Department's Privacy Policy outlines that *"We are permitted to disclose personal information to law enforcement bodies (amongst others) and intelligence bodies for the purpose of enforcing the criminal law, laws imposing a pecuniary penalty or for the purpose of protecting public revenue (amongst other things)"*.
- 5.41 Under APP 6.2(e), the Department is permitted to use or disclose personal information if it reasonably believes that the use or disclosure is 'reasonably necessary' for one or more 'enforcement related activities' conducted by, or on behalf of, an enforcement body.

- 5.42 We understand that personal information collected by the Department may form part of intelligence reporting and constitute IBP Information which may be disseminated to partner agencies where relevant to informing their enforcement related functions.
- 5.43 An entrusted person authorised by the Secretary, may disclose IBP Information containing personal information to another department, agency, AFP or other person or body listed at section 44(4) of the ABF Act if:
- (a) the Secretary is satisfied that the information will enable or assist that body to exercise their powers or functions; and the disclosure is necessary for a purpose listed in section 46, including for example:
 - (i) law enforcement;
 - (ii) protection of public health or safety;
 - (iii) assisting in the establishing of a person's identity;
 - (iv) provision of services to persons who are not Australian citizens;
 - (v) protection of national security or defence of Australia;
 - (vi) locating a missing person; and
 - (vii) purposes relating to matters covered by *Customs Act 1901*, the *Migration Act 1958*, the *Maritime Powers Act 2013*, the *Australian Citizenship Act 2007*, the *Immigration (Guardianship of Children) Act 1946*, the *Education Services for Overseas Students Act 2000* or the *Biosecurity Act 2015*; and
 - (b) the body has complied with any applicable conditions in respect of the disclosure.
- 5.44 In addition, s 51 of the ABF Act provides that disclosure under s 43, 44, 45, 47, 48 or 49 of the ABF Act is taken to be a disclosure that is authorised by the ABF Act, which constitutes a disclosure 'authorised by or under an Australian law' for the purposes of APP 6.2(b). Falling within the APP 6.2(b) exception permits the disclosure of personal information for a purpose other than the purpose for which the information was collected.
- 5.45 We consider these uses and disclosures of personal information are for the primary purpose of border management, community protections, investigations, intelligence and enforcement activities listed in paragraph 4.9 such as investigation and assessment.
- 5.46 Under the *Privacy Act*, if the Department uses or discloses personal information in accordance with the 'enforcement related activities' exception in APP 6.2(e), the Department must make a written note of the use or disclosure (APP 6.5).
- 5.47 'The Department as an Enforcement Body' document provides guidance with respect to the record keeping requirements. We **recommend** that this guidance is provided to all departmental staff who are permitted to use or disclose personal information collected via open-source tools in connection with enforcement related activities. (**Recommendation 4**). The following guidelines should be included:
- (a) the date of the use or disclosure;
 - (b) details of the personal information that was used or disclosed;
 - (c) the enforcement body conducting the enforcement related activity;
 - (d) if the entity used the personal information, how the personal information was used by the entity;

- (e) if the entity disclosed the personal information, who it disclosed the personal information to (this may be the enforcement body or another entity); and
- (f) the basis for the entity's 'reasonable belief'. This will help the entity assure itself that this exception applies, and it may be a useful reference if the entity later needs to justify its reasonable belief.

Cross-border disclosure

- 5.48 An 'overseas recipient' is a person who receives personal information from the Department and is:
- (a) not in Australia or an external Territory;
 - (b) not the Department (disclosing the personal information); and
 - (c) not the individual to whom the personal information relates.
- 5.49 The Department's Privacy Policy identifies that personal information may be disclosed overseas and there may be circumstances where the Department engages contractors to collect, transmit and store data, including providers located outside of Australia.
- 5.50 Under APP 6.1, the Department 'uses' information where it handles or undertakes an activity with the information, within the entity's effective control. Open Source Collection Tools are used within the Department's effective control when the Department directly operates on the tools or provides instructions to the search criteria.
- 5.51 Some of the Open Source Collection Tool providers are based overseas. Once the information from Open Source Collection Tools is collected by the Department's Intelligence Capability, it is stored as an internal departmental record.
- 5.52 Even if the Department engages a third party provider to operate on Open Source Collection Tools, providing personal information to a contractor to perform services on behalf of the Department constitutes a use, rather than a disclosure where the Department does not release the subsequent handling of personal information from its effective control. Given the Department has a binding contract in place with the service providers, which requires the provider only to handle the personal information for limited purposes of performing searches, the Department retains effective control of the personal information and such search requests to a service provider does not constitute a disclosure or overseas disclosure of personal information.
- 5.53 APP 8.1 will not apply to a disclosure of personal information by an APP entity to an overseas recipient where the disclosure is 'required or authorised by or under an Australian law or a court/tribunal order' (APP 8.2(c)). We understand that the Department may also be authorised to disclose personal information to a foreign country, agency or authority of a foreign country or a public international organisation under section 45 of the ABF Act. Such overseas disclosures are in line with the Department's existing BAU disclosure guidance and APP 8.
- 5.54 Under section 45 of the ABF Act, an entrusted person authorised by the Secretary may disclose IBP Information containing personal information to a foreign country, agency or authority of a foreign country or a public international organisation for a purpose mentioned in section 46 of the ABF Act including the purposes set out at paragraph 5.23(a) if:

- (a) The Secretary is satisfied that the information will be used in accordance with an agreement in force between the Commonwealth and that foreign country/agency; and
 - (b) the Secretary is satisfied that the disclosure of that information to that foreign country, agency, authority or organisation is necessary for the purpose mentioned in section 46; and
 - (c) The foreign country, agency, authority or organisation undertakes not to use or further disclose the information except in accordance with the agreement or otherwise as required or authorised by law.
- 5.55 We understand the Department has a number of Memoranda of Understanding (MOU) which set standards of information handling with overseas recipients to ensure the Department is meeting its obligations under the Privacy Act.
- 5.56 Further, APP 8.1 does not apply to cross-border disclosures of personal information where both of the following apply:
- (a) the Department reasonably believes that the disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, and
 - (b) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body (APP 8.2(f)).
- 5.57 The Department is unlikely to have any separate administrative arrangement with the open source tool vendors. Instead, privacy obligations including under APP 8 are passed on to the vendors through the Department's contracts with those vendors.
- 5.58 Prior to overseas disclosure, we understand that departmental personnel, who are permitted to use and disclose the personal information collected via Open Source Collection Tools, should contact the Privacy Operations Section if they require further information about APP 8 per 'The Department as an Enforcement Body' document.
- 5.59 There may be circumstances where personal information collected by each of these Open Source Collection Tools are stored or processed overseas, as follows:

Tool	Storage/processing location
Maltego	Per Article 5 of Maltego's Data Privacy Policy, Maltego may process data obtained from public sources to the extent necessary for the performance of its services. Maltego lists third-party contracts which may process personal information: s. 47G(1)(a) [REDACTED]
Babel Street Insights & Locate X	Per the Privacy Policy, information collected by Babel Street at the instruction of the customer may be processed outside of Australia. The Policy does not list specific locations where Babel Street has facilities or service providers. However, information collected by customers, through Babel Street Insights, is not stored by Babel Street as it is only acting as a 'search engine'.

Sprinklr	Under Spinrklr's Privacy Notice, information collected by Sprinklr at the instruction of the customer may be processed outside of Australia.
ShadowDragon SocialNet	Per ShadowDragon's Privacy Policy, information collected by ShadowDragon through the use of its tools may be stored outside of Australia.
Authentic8 Silo + ToolboxDW	Under Authentic8's Terms of Service, information collected by Authentic8 at the instruction of the customer may be processed outside of Australia.

s. 47(1)(a)

5.60 Although the tools mentioned above have offshore data processes, once the Department collects the information from the tool, we understand it is recorded and stored separately on the Department's systems. The Department stores records of information about individuals on their internal ICT environment which is located onshore in Australia. The Open Source Collection Tools are an intermediary step and no records of personal information are stored on the tools.

5.61

s. 47E(d)

Quality of personal information

5.62 The quality of the information associated with the Project will be dependent on what is publicly available, and in turn, is up to the discretion of Departmental personnel to consider the quality of such information.

5.63 We have not had the opportunity to review any policies or procedures the Department has in place to ensure that the information is accurate, up-to-date and correct.

5.64 We **recommend** the Department satisfy itself that it has appropriate mechanisms (such as standard operating procedures and system controls) to ensure the personal information it holds is accurate, up-to-date and complete and the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (**Recommendation 6**).

Security of personal information

5.65 APP 11 requires the Department to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information.

5.66 The Department must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

5.67 In accordance with the Protective Security Policy Framework (**PSPF**), the Department is required to comply with the Information Security Manual (**ISM**). The PSPF mandates

that all Australian Government agencies, organisations and entities manage the security of their information systems through a certification and accreditation process.

- 5.68 We understand that the use of open-source collection tools has role-based access controls, which require supervisor approval. This includes password protected licences.
- 5.69 We **recommend** the Department satisfy itself that it has appropriate security mechanisms to protect the personal and sensitive information it holds in relation to the Project (**Recommendation 7**).
- 5.70 This could include:
- (a) ICT security mechanisms such as:
 - (iv) encryption;
 - (v) audits and monitoring; and
 - (vi) backup and recovery;
 - (b) internal standard operating procedures;
 - (c) an appropriate Data Breach Response Plan; and
 - (d) destruction and de-identification processes.
- 5.71 We understand that where required, a Security Impact Assessment is conducted with the Department's Cyber Risk Management Branch during the procurement process for open source tools.
- 5.72 We **recommend** the Department obtain a Security Risk Assessment (**SRA**) relating to the Project and consider implementing any recommendations forming part of the SRA (**Recommendation 8**).
- 5.73 We understand that all Departmental staff are required to complete the Essentials Suite, which is mandatory training about privacy and personal information, and associated obligations. Additionally, we understand that Departmental staff are regularly required to complete security awareness training.

Storage, retention and destruction of personal information

- 5.74 The Department must take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs.
- 5.75 However, this requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information (APP 11.2). Under APP 11.2 and the *Archives Act 1983* (Cth) (**Archives Act**), Australian Government agencies such as the Department are generally required to retain the personal information they hold as 'Commonwealth records', for the periods specified in the relevant Records Authority made under the Archives Act. The Archives Act makes it an offence to destroy a Commonwealth record before expiration of its retention period (section 24).
- 5.76 Storage and retention of personal and sensitive information collected by open-source tools used by the Department must be in accordance with the Department's Protective Marking and Handling of Sensitive and Security Classified Information Procedural

Instruction (HR-6361), which adheres to the broader Protective Security Policy Framework (PSPF), and relevant legislation.

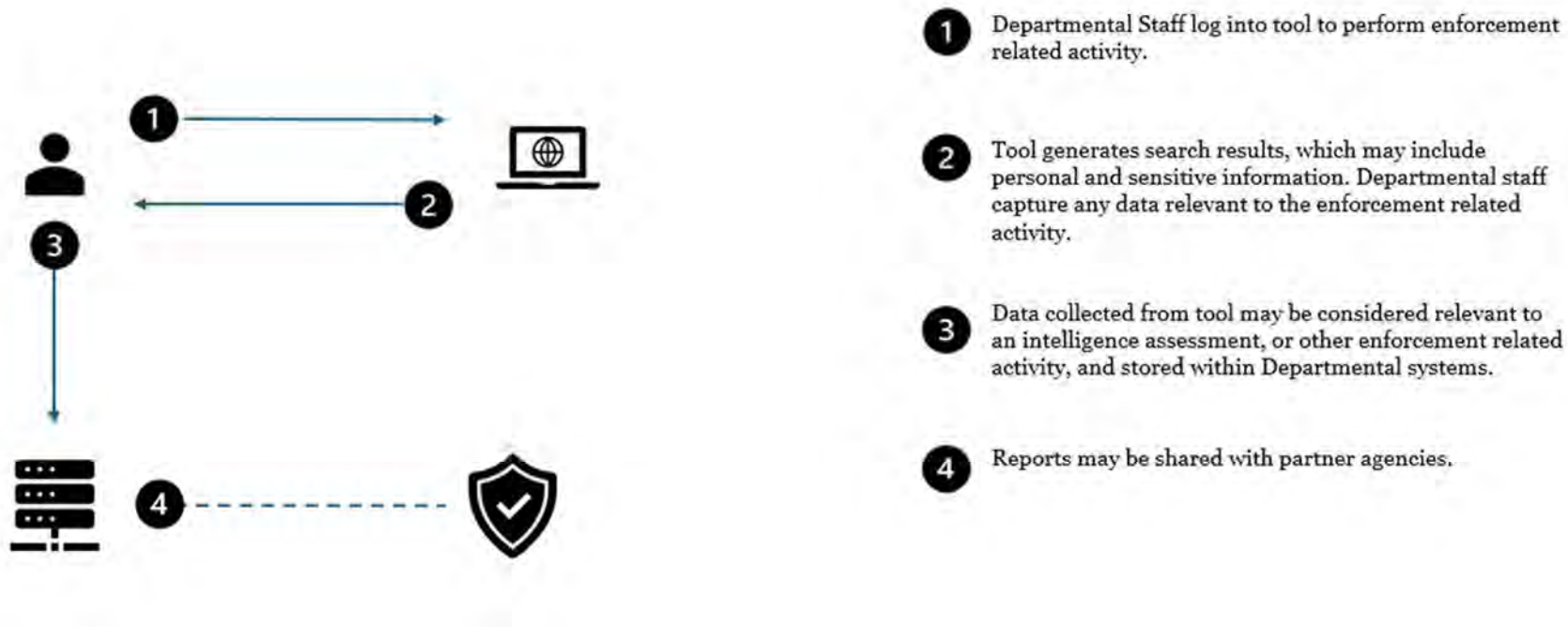
- 5.77 We understand that bulk data provided by the use of the open source tools is not extracted by the Department. Where information is relevant to an intelligence assessment, it is manually collated by Departmental Staff and stored as part of the information base for the work being undertaken. Any resulting artefacts are stored in Departmental record keeping systems at the level of PROTECTED or higher.
- 5.78 We **recommend** the Department retain the records associated with the Project per existing Departmental records management protocols and the Records Authorities that apply to the Department's core activities (**Recommendation 9**).

Access to and correction of personal information

- 5.79 As each open-source tool collects data from publicly available information on the internet, and not the individual themselves, there will be no opportunity for correction.
- 5.80 When exercising its law enforcement functions, the Department may not be required to provide an individual access to the personal information under APP 12.2 and s 37 of the FOI Act if the Department can provide evidence that providing access to information collected via open-source tools would affect enforcement of law and protection of public safety.
- 5.81 Information falling under Part IV, Division 2 of the FOI Act may also be exempted, such as information relating to national security, defence or international relations (s 33), cabinet documents (s 34) and information subject to legal professional privilege (s 42). A conditional exemption in Part IV Div 3 may also apply depending on the circumstances.
- 5.82 A decision to refuse access under APP 12.2(b)(i) (on one of the FOI grounds) is a decision made under the Privacy Act, not the FOI Act. As required by APP 12.9, the Department must provide the individual with a written notice that sets out the reasons for the refusal and the complaint mechanisms available to the individual. The individual may have a right to complain to the Information Commissioner under the Privacy Act. After investigation, the Commissioner may make a determination that the Department has failed to comply with APP 12 and require, for example, that the agency give access (Privacy Act, s 52). However, the individual will not have a right to seek internal review or Information Commissioner review under the FOI Act.

Flow of information

5.83 An illustration of information flows associated with the Project is in **Annexure A**.



OFFICIAL: SENSITIVE

PART 6: COMPLIANCE WITH THE APPS

6.1 We have considered compliance of the Project against each of the APPs in preparing this PIA. Our analysis refers only to the specific Project with respect to the Department's compliance with the APPs, and not any broader analysis of the APPs.

C	Compliant
CI	Compliant, but could be improved
NC	Non-compliant

Australian Privacy Principle	Rating	Details/comments
APP 1 – open and transparent management of personal information	CI	APP 1 requires the Department to manage personal information in an open and transparent way; take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs; and to have a privacy policy which covers a range of prescribed matters. The Department's Privacy Policy is publicly available at Privacy (homeaffairs.gov.au). The Privacy Policy explains how the Department collects and handles personal information, and how an individual can access or correct their personal information or submit a complaint. The Department has mentioned in its Privacy Policy Section 4 that it may collect personal information for the following purposes: border management, visa compliance and immigration status resolution, certain Australian laws including criminal and community protection, and enforcement related activities such as detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law. The Department's Privacy Policy identifies that personal information may be collected from other sources, such as publicly available sources. However, the Privacy Policy does not specifically call out the methods by which the Department utilises to collect personal information from publicly available sources. While APP 1.4(b) states that the

OFFICIAL: SENSITIVE

		usual approach to collecting personal information must be explained in the Privacy Policy, to strengthen compliance with APP 1, in furtherance of accountability and transparency, we recommend the Department include how personal information is collected via open-source collection tools and ensure all the primary collection purposes have been included in the Privacy Policy (see Recommendation 2).
APP 2 – anonymity and pseudonymity	N/A	APP 2 requires that individuals are given the opportunity to remain anonymous or use a pseudonym, unless it is not practicable, or there is a legal reason why this cannot happen. APP 2.2(b) provides that an individual may not have the option of dealing anonymously or by pseudonym with an APP entity if 'it is impracticable for the APP entity to deal with individuals who have not identified themselves'. Given the nature of the Project, we conclude it is not practical for the Department to allow individuals to interact with the Department on a pseudonymous or anonymous basis.
APP 3 – collection of solicited personal information	CI	APP 3 states that when the Department collects personal information, that collection should be reasonably necessary for, or directly related to, one of the Department's functions. Personal information should also be collected directly from the individual concerned unless it is impractical to do so and by lawful and fair means. APP 3 also sets out the restrictions on collecting sensitive information for agencies. The information collected for the Project is reasonably necessary for, and directly related to the Department's functions and activities. In line with the Department's 'Online Open Source and Social Media Access Policy', we consider the Department's use of the open-source tools to be consistent with this requirement. The Department's functions are conferred either by legislation or an executive scheme or arrangement established by government. The legislation which governs the use of Open Source Collection Tools by the Department are listed in paragraph 4.5 of the Open Source Collection Tools PIA.

OFFICIAL: SENSITIVE

		Any collection, use or disclosure of materials from Open Source Collection Tools by the Intelligence Capability will be considered on a case-by-case basis to assess its collection purpose. We understand that personal information collected by the Department may form part of intelligence reporting and constitute IBP Information for the purposes of the ABF Act s 4, which may be disseminated to partner agencies where relevant to informing their enforcement related functions. If the Department collects information for purposes other than s 16A exception activities and enforcement related activities, the Department collects, uses and discloses personal information for the primary purposes of border management, community protections, investigations, intelligence and enforcement activities listed in paragraph 4.9 such as investigations and assessment. The Department should be mindful when using Open Source Collection Tools for purposes outside of the enforcement activities and s 16A exception activities and ensure compliance with APP 3. We believe Recommendation 3 will improve the Department's compliance with APP 3.
APP 4 – dealing with unsolicited personal information	C	APP 4 outlines the steps an APP entity must take if it receives unsolicited personal information. If an APP entity receives unsolicited personal information, it must decide whether it could have collected the information under APP 3 (collection of solicited personal information). If the entity could not have collected the personal information and the information is not contained in a Commonwealth record – the entity must destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so (APP 4.3). We understand that while search requests within the tools can provide search results that may include personal information, including sensitive information, which is not necessary for the functions of the Department, only the information that is relevant to an investigation is collected by the Department. No unsolicited personal information is expected to be collected for this Project.

OFFICIAL: SENSITIVE

APP 5 – notification of the collection of personal information	C	APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. The Department has mentioned in its Privacy Policy Section 4 that it may collect personal information for the following purposes: border management, visa compliance and immigration status resolution, certain Australian laws including criminal and community protection, and enforcement related activities such as detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law. We are satisfied the Department complies with requirements outlined in APP 5.
APP 6 – use or disclosure of personal information	CI	APP 6 states that the Department can only use or disclose personal information for the purpose for which it was collected (known as the ‘primary purpose’) or for a secondary purpose if the individual has provided their consent or an exception applies. The Department’s Privacy Policy outlines that “we are permitted to disclose personal information to law enforcement bodies (amongst others) and intelligence bodies for the purpose of enforcing the criminal law, laws imposing a pecuniary penalty or for the purpose of protecting public revenue (amongst other things)”. In this Project, the Department collects, uses and discloses personal information for the primary purposes of border management, community protections, investigations, intelligence and enforcement activities listed in paragraph 4.9 such as investigation and assessment. The specific purpose applicable to a particular use of a Tool depends on the circumstances. The Department’s primary use of personal information is aligned with the collection purposes outlined in its privacy policy and therefore is compliant to APP 6.1. The Department may also use personal information for secondary purposes beyond the original collection purpose, such as for research and reporting purposes. If the Department uses Open Source Collection Tools for purposes beyond the primary purposes and relies on APP 6.2 as an exception, the Department needs to be mindful

OFFICIAL: SENSITIVE

		that for any use and disclosure purposes beyond the primary purposes, the secondary use and disclosure purpose must fall within one of the exceptions outlined in the APP 6.2: (a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose, and the secondary purpose is directly related the primary purpose (if the information is sensitive information), or related to the primary purse (if the information is personal information); (b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; (c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; (d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; (e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body. In this Project, APP 6.2(b) may apply when the Department operates under a court order or where it is otherwise authorised or required by law. APP 6.2 (c) may apply to publicly available information that has been collected by the Department using Open Source Collection Tools if the use or disclosure of the information falls within one of the s 16A exceptions. We understand that personal information collected by the Department may form part of intelligence reporting which may be disseminated to partner agencies where relevant to informing their enforcement related functions. Under the Privacy Act, if the Department uses or discloses personal information in accordance with the 'enforcement related activities' exception in APP 6.2(e), the Department must make a written note of the use or disclosure (APP 6.5). Additionally, if the Department discloses personal information contained within IBP Information, the disclosure must be in accordance with an exception under s 42(2) of the ABF Act, such as sections 44(2) and s 45(2) of the ABF Act.
--	--	---

OFFICIAL: SENSITIVE

		As discussed with Recommendation 4 , 'The Department as an Enforcement Body' document provides guidance with respect to the record keeping requirements. We believe this recommendation will improve the Department's compliance with APP 6.
APP 7 – direct marketing	NA	The Department is not required to comply with APP 7, as the Department is not listed in Part 1 of Schedule 2 of the <i>Freedom of Information Act 1982 (FOI Act)</i> and the Department's functions are not related to a commercial activity.
APP 8 – cross-border disclosure of personal information	CI	APP 8 requires the Department to take reasonable steps to ensure that overseas recipients do not breach the APPs in relation to any personal information disclosed to them. The Department's Privacy Policy identifies that personal information may be disclosed overseas and there may be circumstances where the Department engages contractors to collect, transmit and store data, including providers located outside of Australia. Under APP 6.1, the Department 'uses' information where it handles or undertakes an activity with the information, within the entity's effective control. The Open Source Collection Tools are used within the Department's effective control when the Department directly operates on the tools or provides instructions to the search criteria. Some of the Open Source Collection Tool providers are based overseas. Once the information from Open Source Collection Tools is collected by the Department's Intelligence Capability, it is stored as an internal departmental record. Even if the Department engages a third party provider to operate on Open Source Collection Tools, providing personal information to a contractor to perform services on behalf of the Department constitutes a use, rather than a disclosure where the Department does not release the subsequent handling of personal information from its effective control. Given the Department has a binding contract in place with the service providers, which requires the provider only to handle the personal information for limited purposes of performing searches, the Department retains effective control of the personal information and such search requests to a service provider does not constitute a disclosure or overseas disclosure of personal information.

OFFICIAL: SENSITIVE

		We understand that the Department may also be authorised to disclose personal information to a foreign country, agency or authority of a foreign country or a public international organisation under s 45 and s 46 of the Australian Border Force Act 2015 (Cth). Such overseas disclosures are in line with the Department's existing BAU disclosure guidance and APP 8. Further, APP 8.1 does not apply where both of the following apply: (a) the Department reasonably believes that the disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, and (b) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body (APP 8.2(f)). Prior to overseas disclosure, we understand that Departmental personnel, who are permitted to use any disclose the personal information collected via Open Source Collection Tools, should contact the Privacy Operations Section if they require any further information on APP 8, per 'The Department as an Enforcement Body' document. We recommend the Department implement Recommendation 5 to improve compliance with APP 8.
APP 9 – adoption, use of disclosure of government related identifiers	NA	The Department is not required to comply with APP 9, as the Department is not listed in Part 1 of Schedule 2 of the FOI Act.
APP 10 – quality of personal information	CI	The quality of the information associated with the Project will be dependent on what is publicly available, and in turn, is up to the discretion of Departmental personnel to consider the quality of such information. We have not had the opportunity to review any policies or procedures the Department has in place to ensure that the information is accurate, up-to-date and correct.

OFFICIAL: SENSITIVE

		As discussed in Recommendation 6 , we would advise the Department satisfy itself that it has appropriate mechanisms to ensure the personal information it holds is accurate, up-to-date and complete and the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.
APP 11 – security of personal information	CI	APP 11 requires the Department to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. The Department must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. In accordance with the Protective Security Policy Framework (PSPF), the Department is required to comply with the Information Security Manual (ISM). The PSPF mandates that all Australian Government agencies, organisations and entities manage the security of their information systems through a certification and accreditation process. We understand that the use of open-source collection tools has role-based access controls, which require supervisor approval. This includes password protected licences. To ensure compliance we have suggested Recommendations 7, 8 and 9. We recommend the Department satisfy itself that it has appropriate security mechanisms to protect the personal and sensitive information it holds in relation to the Project, and retain records associated with the Project per existing Departmental records management protocols and the Records Authorities that apply to the Department's core activities.

OFFICIAL: SENSITIVE

		We believe the Department should also obtain a Security Risk Assessment (SRA) relating to the Project and consider implementing any recommendations forming part of the SRA. We understand that all Departmental staff are required to complete the Essentials Suite, which is mandatory training about privacy and personal information, and associated obligations. Additionally, we understand that Departmental staff are regularly required to complete security awareness training.
APP 12 – access to personal information	C	APP 12 requires the Department provide individuals with access to their personal information on request. The Department can refuse this access, but only under certain grounds. If access is refused, written notice must be provided, along with complaint mechanisms available to an individual. When exercising its law enforcement functions, the Department may not be required to provide an individual access to the personal information under APP 12.2 and s 37 of the FOI Act, if the Department can evidence that providing access to information collected via open-source tools would affect enforcement of law and protection of public safety. Information falling under Part IV, Division 2 of the FOI Act may also be exempted, such as information relating to national security, defence or international relations (s 33), cabinet documents (s 34) and information subject to legal professional privilege (s 42). A conditional exemption in Part IV Div 3 may also apply in some circumstances. A decision to refuse access under APP 12.2(b)(i) (on one of the FOI grounds) is a decision made under the Privacy Act, not the FOI Act. As required by APP 12.9, the Department must provide the individual with a written notice that sets out the reasons for the refusal and the complaint mechanisms available to the individual.

OFFICIAL: SENSITIVE

APP 13 – correction of personal information	C	APP 13 requires the Department to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. As each open-source tool collects data from publicly available information on the internet, and not the individual themselves, there will be no opportunity for correction. Further, in light of the Department's enforcement related activities, there will be no opportunity for individuals to request correction.
--	----------	---

PART 7: PRIVACY IMPACT ANALYSIS AND COMPLIANCE CHECK

- 7.1 The PIA Guide recommends agencies analyse how a project impacts privacy, both positively and negatively. This is broader than simply assessing the project for compliance with the APPs.

Whether additional safeguards are required to ensure that the privacy interests of individuals are appropriately protected?

- 7.2 We have set out in paragraph 2.1 of this PIA a number of recommendations which we believe if implemented will manage the privacy interests of individuals as part of the Project.

Additional compliance questions

- 7.3 In considering the broader privacy impacts, the PIA Guide poses some key questions. The questions relevant to the Project are addressed below.

Do individuals have to give up control of their personal information?

- 7.4 Individuals do not give up control of their personal information, as what is collected by the Department is available from publicly available sources. Because of the legal and law enforcement framework within which the Department operates, its use and disclosure of personal information is highly circumscribed and, in some cases, carries criminal penalties for misuse.

Will the Project change the way individuals interact with the Department, such as through more frequent identify checks, costs or impacts on individuals or groups who do not have identity documents?

- 7.5 No, the Project does not involve direct interaction with individuals.

Will decisions that have consequences for individuals be made as a result of the way personal information is handled in the Project (such as decisions about services or benefits)?

- 7.6 It depends on how the Department uses this information and the purpose of the Department's original search. The information is being collected from publicly available sources.

Is there a complaint-handling mechanism? If yes, is it visible, comprehensive and effective?

- 7.7 The Department's Privacy Policy outlines the Department's complaint-handling mechanism which gives complainants the option of direct complaint or escalation to the OAIC. Further, the Department's online complaints form provides a range of means to raise privacy complaints directly to the Department.
- 7.8 The Privacy Policy confirms that complainants will be advised of complaint outcomes and that complaints will be dealt with quickly and fairly.

How will the Department handle any privacy breaches?

- 7.9 Privacy breaches are managed in accordance with the Department's existing Privacy breaches and Notifiable Data Breaches Scheme document.
- 7.10 We **recommend** the Department ensures its Data Breach Response Plan appropriately considers information handling associated with the Project, to ensure that privacy breaches are identified and mitigated in a timely manner (**Recommendation 10**).

Are there audit and oversight mechanisms in place (including emergency procedures) in case the system fails?

- 7.11 In addition to data breach management (as discussed immediately above), the Department is obliged to comply with the ISM (including its guidelines for Cybersecurity incidents, physical and personnel security, system hardening, ICT equipment, system management and monitoring, database systems and data transfers). It is also required to follow the [Information Security Policies](#) of the PSPF, covering 'Sensitive and classified information' (Policy 8), 'Access to information' (Policy 9), 'Safeguarding data from cyber threats' (Policy 10) and 'Robust ICT Systems' (Policy 11).
- 7.12 This obligation is not changed by the implementation of the Project. Accordingly, the Department's existing business continuity and emergency management arrangements continue to apply.

Does the Project recognise the risk of function creep? (For example, is there an interest in using the personal information collected for the project for other purposes that might occur in the future?)

- 7.13 Yes, there is a risk of function creep if the Department plans to collect, use and disclose information for additional secondary purposes outside of the primary and secondary purposes recognised in this PIA. If the Department collects information for purposes other than s 16A exception activities and enforcement related activities, the Department collects, uses and discloses personal information for purposes of border management, community protections, investigations, intelligence and enforcement activities listed in paragraph 4.9 such as investigations and assessment.
- 7.14 Most of these collection purposes require s. 47G(1)(a) and the Department will assess on a case-by-case basis to consider whether it would be unreasonable or impracticable to collect information directly from individuals to avoid jeopardising the collection purposes.
- 7.15 As discussed with **Recommendation 4**, 'The Department as an Enforcement Body' document provides guidance with respect to the record keeping requirements. We believe this recommendation will mitigate the risk of function creep.

How valuable would the information be to unauthorised users? (For example, is it information that others would pay money for or try to access via hacking?)

- 7.16 The information would be highly valuable to unauthorised users as it may contain intelligence reports based on key identity information or sensitive information of individuals. However, the Department has identified this as a risk and has appropriate security mechanisms in place to ensure personal information is protected.

Is any intrusion or surveillance fully justified and in proportion to the Project's anticipated benefits? Is it the only way of achieving the aims of the Project, and

done in the least intrusive manner? Is it subject to legislative or judicial authority? What auditing and oversight measures are in place?

- 7.17 The Project uses information collected by the Department from publicly available sources and we have made previous recommendations to the Department to be aware of collection by lawful and fair means without intimidation, deception or use of means that are unreasonably intrusive, especially when the Department collects and uses information for purposes outside the s 16A exceptions or enforcement related activities.
- 7.18 We note that collecting and using personal information for purposes within the S 16A exceptions and for enforcement related activities are subject to exceptions, and any intrusion is limited to what is necessary for the enforcement related activities.
- 7.19 As a privacy-positive strategy, we **recommend** a post-implementation audit after the deployment of the Project to assess whether any changes need to be made to functionality or processes to better protect the data (**Recommendation 11**). The Department may decide a practical timeframe for the post-implementation audit considering other changing factors, such as policy updates.

How consistent is the project with community values about privacy?

- 7.20 The OAIC has published the *Australian Community Attitudes to Privacy Survey 2023 (OAIC 2023 survey)*. Relevantly, the OAIC survey found:
- (a) 74% of respondents feel data breaches are one of the biggest privacy risks they face. This has increased by 13% since 2020; and
 - (b) Federal government agencies were rated second in the level of trustworthiness by sector – with 67% of respondents rating Federal government agencies as ‘somewhat trustworthy’ or ‘very trustworthy’.
- 7.21 In addition, the previous OAIC *Australian Community Attitudes to Privacy Survey 2020 (OAIC 2020 survey)* identified that:
- (a) 70% of respondents were uncomfortable with government agencies sharing their personal information with businesses in Australia; and
 - (b) 40% of respondents felt that the privacy of their personal information was either poorly or very poorly protected.’

PART 8: ASSESSMENT OF DEPARTMENT PRIVACY POLICY

8.1 We have reviewed the Department's Privacy Policy (last updated 31 May 2023) for compliance against the APPs. We have considered whether the specific matters prescribed by APP 1 are incorporated into the Department's Privacy Policy:

Compliance check	Requirement	Comments
✓	The kinds of personal information that the entity collects and holds	The Privacy Policy comprehensively lists the information collected by the Department in contexts such as visa and migration, refugee and humanitarian assistance, and border management.
✓	How the entity collects and holds personal information	The Policy lists interviews, application forms and other official forms as the sources from which it collects personal information. The Privacy Policy also provides for the collection of personal information from other sources, including third parties such as other government agencies and members of the public.
✓	The purposes for which the entity collects, holds, uses and discloses personal information	The Privacy Policy clearly sets out the purposes for which the Department collects different types of personal information. A full list of the Department's programmes as well as its administrative and enforcement related activities is provided to complement reference to the Department's 'functions or activities' as the primary purpose of collecting personal information. The Privacy Policy notes that the Department will also disclose personal information to facilitate merits or judicial review of a decision.
✓	Clearly expressed that is easy to understand	The Privacy Policy does not include notably legalistic wording or jargon.
✓	Tailored to the specific information handling practices of the entity	The level of detail provided in the Privacy Policy indicates that the policy is tailored to the information handling procedures of the Department.
✓	Privacy Policy available free of charge in an appropriate format	The Privacy Policy is publicly available for free through the Department's website.

Compliance check	Requirement	Comments
✓	How an individual may access personal information about the individual that is held by the entity and seek the correction of such information	The Privacy Policy provides a link to Form 424A for access to personal information held by the Department. It also lists the governing legislation of access procedures. Correction procedures are detailed thoroughly, and numerous forms and explanations are provided to account for the circumstances of Australian and non-Australian citizens seeking correction to personal information held by the Department.
✓	How an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint	The Privacy Policy provides an online feedback form as well as the addresses of the Department's Global Feedback Unit and the OAIC. The Privacy Policy notes that the OAIC would likely recommend that a person try to resolve the complaint directly with the Department in the first instance. The Privacy Policy provides that complaints "will be investigated and complainants will be advised of the outcome".
✓	Whether the entity is likely to disclose personal information to overseas recipients	The Policy provides a thorough outline of the circumstances in which personal information may be disclosed to overseas recipients by the Department or its contractors.
✓	If the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy	No details are provided of the location of overseas personal information recipients in the Policy. We understand that the operational sensitivity of the Department means that incorporating this information may be impractical.

ANNEXURE A: GLOSSARY

Throughout this PIA, the following terms have the corresponding meaning:

ABF	Australian Border Force
AI	Artificial Intelligence
APIs	Application Programming Interfaces
APP Code	<i>Privacy (Australian Government Agencies – Governance) APP Code 2017</i> . The APP Code is a written code, developed for the handling of personal information, available at: Privacy (Australian Government Agencies – Governance) APP Code 2017 OAIC
APP	The Australian Privacy Principles as set out in Schedule 1 of the <i>Privacy Act 1988</i> .
APP Guidelines	The OAIC's publication <i>Australian Privacy Principles Guidelines</i> , available at Australian Privacy Principles guidelines OAIC
Archives Act	<i>Archives Act 1983</i> (Cth)
CRM	Customer Relationship Management
Department	Department of Home Affairs
DNS	Domain Name System
Division	Department of Home Affairs (former) Intelligence Division
FOI Act	<i>Freedom of Information Act 1982</i> (Cth)
GL	Griffin Legal
GPT	Generative Pre-training Transformer
Health Information Section 6FA, <i>Privacy Act</i>	(a) information or an opinion about: (i) the health, including an illness, disability or injury, (at any time) of an individual; or (ii) an individual's expressed wishes about the future provision of health services to the individual; or (iii) a health service provided, or to be provided, to an individual;

Released by Department of Home Affairs
Under the Freedom of Information Act 1982

	that is also personal information; (b) other personal information collected to provide, or in providing, a health service to an individual; (c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances; (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.
Intelligence Capability	The Department's dispersed intelligence teams formerly contained in the Intelligence Division
ISM	Information Security Manual
IoT	Internet of Things
OSINT	Open Source Intelligence
OGI	Online and Geospatial Intelligence Section
OAIC	Office of the Australian Information Commissioner
OAIC 2020 survey	The OAIC's publication <i>Australian Community Attitudes to Privacy Survey 2020</i> , available at Australian Community Attitudes to Privacy Survey 2020 OAIC
OAIC 2023 survey	The OAIC's publication <i>Australian Community Attitudes to Privacy Survey 2023</i> , available at Australian Community Attitudes to Privacy Survey 2023 OAIC
Personal Information, Section 6, <i>Privacy Act</i>	information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
PIA Section 33D(3), <i>Privacy Act</i>	A privacy impact assessment is a written assessment of an activity or function that: (a) identifies the impact that the activity or function might have on the privacy of individuals; and (b) sets out recommendations for managing, minimising or eliminating that impact.
PIA Guide	The OAIC's publication <i>Guide to undertaking privacy impact assessments</i> , available at: Guide to undertaking privacy impact assessments OAIC
Privacy Act	<i>Privacy Act 1988</i> (Cth)

Privacy Policy	The Department's Privacy Policy, available at Privacy (homeaffairs.gov.au)
Project	Open-Source Collection Tools
PSPF	Protective Security Policy Framework
SaaS	Software as a Service
SRA	Security Risk Assessment
Sensitive Information – Section 6, <i>Privacy Act</i>	(a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.
VPC	Virtual Private Cloud

OFFICIAL: SENSITIVE

griffinlegal.



Australian Government
Department of Home Affairs

Department of Home Affairs
Open-source collection tools –
Additional Tools

Privacy Impact Assessment Addendum

FINAL

1 April 2025

Released by Department of Home Affairs
under the Freedom of Information Act 1982