CONTENTS

PART 1: EXECUTIVE SUMMARY 4

PART 2: RECOMMENDATIONS AND DEPARTMENT'S RESPONSE 5

PART 3: METHODOLOGY AND ASSUMPTIONS 11

PART 4: PROJECT DESCRIPTION 12

PART 5: COMPLIANCE WITH THE APPS 26

PART 6: PRIVACY IMPACT ANALYSIS AND COMPLIANCE CHECK 49

ANNEXURE A: GLOSSARY 52

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

REFERENCE SCHEDULE

Name of Project	Additional Open-source Collection Tools Addendum		
Name of Client	The Department of Home Affairs		
Date	1 April 2025	**PIA version number**	v.03
PIA prepared by	s. 47F(1) Griffin Legal	**Contact details**	s. 47F(1)
Client project manager	s. 22(1)(a)(ii)	**Contact details**	s. 22(1)(a)(ii)

VERSION HISTORY

Version	Date	Summary of changes
v.01	16 December 2024	Initial Addendum PIA provided to the Department
v.02	25 February 2025	Updated Addendum PIA based on further comments
v.03	1 April 2025	Final PIA based on further Feedback on ILS 25 March 2025

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

PART 1: EXECUTIVE SUMMARY

Overview

1.1 In September 2024, Griffin Legal (GL) completed a Privacy Impact Assessment (**PIA**) for Open Source Collection Tools Project for the Department.

s. 47(1)(a)

(b) FiveCast Onyx;

(c) OIS (Online Investigation Suite);

(d) Orbis (Moody's Analytics);

(e) Web of Science; and

(f) Sayari,

(the **Project**).

1.3 It is our view that the privacy risks associated with the additional tools utilised by the Project can be appropriately managed and mitigated in accordance with the recommendations in this Addendum PIA.

1.4 This Addendum 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 5 – Compliance with the APPs**.

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

PART 2: RECOMMENDATIONS AND DEPARTMENT'S RESPONSE

Summary of recommendations

2.1 This PIA makes **41 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 the recommendations of the PIA – Open Source Collection Tools project dated 11 September 2024, which apply to all open source tools (paragraph 4.4).	
		OSINT Combine NexusXplore	
2.	**APP 1**	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 the assistance of software and ensure all the primary collection purposes have been included in the Privacy Policy.	
3.	**APP 1**	To prepare for the upcoming Privacy Act changes, we **recommend** the Department include in its Privacy Policy that computer programs are used to assist with intelligence gathering, investigations, research and reporting purposes.	
4.	**APP 6**	We **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conduct a research).	
5.	**APP 6**	s. 37(2)(b)	

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

6.	APP 10	s. 37(2)(b)
7.	APP 11	
	Fivecast Onyx	
8.	APP 1	s. 37(2)(b)
9.	APP 1	
10.	APP 1	
11.	APP 3	
12.	APP 6	
13.	APP 6	
14.	APP 6	

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

		database and set up storage locations internal to the Department to keep personal information and confidential information.	
15.	**APP 10**	We **recommend** the Department cross reference and verify search results from Onyx before relying on it.	
16.	**APP 11**	s. 37(2)(b)	
		OIS	
17.	**APP 6**	As mentioned above, we **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conducting a research).	
		Orbis	
18.	**APP 1**	As mentioned above, we **recommend** the Department include how personal information is collected from online open sources including the assistance of software and ensure all the primary collection purposes of using Orbis have been included in the Privacy Policy.	
19.	**APP 1**	We **recommend** the Department understand how AI works in the search process, and incorporating the use of AI in the Department's Privacy Policy.	
20.	**APP 6**	As mentioned above, we **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conducting a research).	
21.	**APP 6**	s. 37(2)(b)	
22.	**APP 6**	We **recommend** the Department identify: (a) the location where information such as search results will be retained; (b) how long the retention period will be;	

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

		(c) the cloud environment where data will be retained and whether it is a secure environment; (d) from which countries Orbis staff can access data from; (e) for what purposes can Orbis staff access the Department's customer data, and whether Orbis is required to notify the Department; (f) whether third parties engaged by Orbis may have access to the Department's customer data, and whether Orbis is required to notify the Department. Once the Department has this information, we **recommend** the Department develop operational procedures to minimise the amount of data stored in Orbis and set up internal report storage locations to keep personal information and confidential information in the Department's internal storage in Australia.	
23.	**APP 10**	We **recommend** the Department cross reference and verify search results from Orbis before relying on it.	
24.	**APP 11**	s. 37(2)(b)	
25.	**APP 11**	We also **recommend** a further PIA be conducted if any integrations were to take place to prevent function creep (e.g. Enterprise Data Warehouse (EDW)).	
		Web of Science	
26.	**APP 1**	As mentioned above, we **recommend** the Department include how personal information is collected from online open sources including the assistance of software and ensure all the primary collection purposes of using Web of Science have been included in the Privacy Policy.	
27.	**APP 1**	We **recommend** the Department understand how AI works in the search process, and incorporating the use of AI in the Department's Privacy Policy.	
28.	**APP 6**	As mentioned above, we **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP	

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

		6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conducting a research).	
29.	**APP 6**	s. 37(2)(b)	
30.	**APP 10**	We **recommend** the Department cross reference and verify search results from Web of Science before relying on it.	
31.	**APP 11**	s. 37(2)(b)	
32.	**APP 11**	Given function restrictions in place, we **recommend** the Department always log in as a 'Personalised User' for audit and tracking purposes.	
33.	**APP 11**	s. 37(2)(b)	
		Sayari	
34.	**APP 1**	As mentioned above, we **recommend** the Department include how personal information is collected via Sayari and ensure all the primary collection purposes of using Sayari have been included in the Privacy Policy.	
35.	**APP 1**	We **recommend** the Department understand how AI functions in Sayari impact the search process, and incorporating the use of AI in the Department's Privacy Policy.	
36.	**APP 6**	As mentioned above, we **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conduct a research).	
37.	**APP 10**	We **recommend** the Department cross reference and verify search results from Sayari before relying on it.	
38.	**N/A**	We **recommend** the Department ensures its Data Breach Response Plan appropriately considers information handling associated with the Project, to	

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

		ensure privacy breaches are identified and mitigated in a timely manner (Paragraph 66.14).	
39.	**N/A**	We **recommend** the Department regularly conduct security audit and third-party security assessments on the Open Source Collection Tools in case of updates and new functions and features being added to the tools (Paragraph66.17).	
40.	**N/A**	There is a risk of "function creep" where there is an expansion in the purposes for which personal information associated with the Project is used or disclosed (that is, for secondary purposes not initially anticipated). We **recommend** the Department implement processes and governance arrangements to ensure function creep does not occur, such as periodic reviews that information collected in respect of the Project continues to be used by the Department solely for the primary purpose of collection (Paragraph 66.18).	
41.	**N/A**	As a privacy-positive strategy, we **recommend** a post-implementation audit six months after the deployment of the Project to assess whether any changes need to be made to functionality or processes to better protect the data (Paragraph 66.22).	

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

PART 3: METHODOLOGY AND ASSUMPTIONS

3.1 The methodology for completing this Addendum PIA is the same as stated in **Part 3** of **PIA – Open Source Collection tools dated 1 April 2025.**

Assumptions and limitations

3.2 GL has prepared this Addendum PIA in consultation with the Department.

3.3 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 and in the documents listed in paragraph 3.7 accurately reflect the Project.

3.4 GL has been engaged to undertake this Addendum PIA at the instruction of the Department and considered only the Department's handling of personal information with respect to the Project.

3.5 Any documents referring to the Department of Border Protection will be considered as the equivalent of the Department of Home Affairs as the *Acts Interpretation Act* and the *Administrative Arrangements Orders* capture any Machinery of Government (MoG) / Portfolio name change.

3.6 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

3.7 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;

(c) (Orbis) - MA Information Security FAQs;

s. 47(1)(a)

(e) Maltego and Information Flows.

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

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

4.2 The background of the Project is as stated in **Part 4** of **PIA – Open Source Collection Tools dated 1 April 2025**.

4.3 On 11 July 2024 the Department notified GL that a number of open source vendors were not included in the scope of work for **PIA – Open Source Collection Tools dated 1 April 2025.** This Addendum PIA covers the additional six tools the Department are using.

4.4 We **recommend** the Department implement the recommendations of the PIA – Open Source Collection Tools project dated 11 September 2024, which apply to all open source tools (**Recommendation 1**).

s. 47(1)(a)

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

(b) Geospace Intelligence – can extract geographic-specific content, such as satellite imagery, social media, news, radio stations, air and marine traffic and location signals data.

4.10 The NexusXplore platform does not store any data other than log-in credentials required to access the platform and search criteria entered by the customer unless the persistent monitoring feature of the Platform is utilised by the customer. Where this feature is utilised, the Platform will store the data from customer's searches for a period of 12 months. This data can only be accessed by the customer.

4.11 The Platform has the capability to search and gather publicly and commercially available information on a large scale, and to match and combine datasets according to the customer request. Artificial intelligence is not used in the information searching and gathering process.

4.12 NexusXplore also has the following capabilities which will be utilised by the Department:

(a) Visual Analysis – conduct cross-platform social network analysis and pattern recognition, including rapid visualisation of platform or key user datapoints;

(b) Cyber Toolbox – capability to search names, emails, phone numbers, IP and physical addresses, usernames and breached credentials;

(c) Grey Literature – locate global research papers and patents informing contemporary scientific and technological developments;

(d) Safe Research Portal – provides an embedded managed attribution system which allows the analyst to manipulate their digital footprint to mask their identity, location and intent to browse the wider internet with added security and a different perceived online persona;

(e) Public and Corporate Records – access to 8+ billion public/person records and 400+ million company records globally, including ownership, trade and asset data;

(f) Dark Web – secure in-platform access to dark web content from 2014 and access to TOR network via a non-attributable, secure browser for safe and live dark web access; and

(g) Country & Travel Briefs – Robust reporting of aggregate and processed country and travel information from different sources.

4.13 The Customer will be solely responsible for determining:

(a) the types of information that it intends to use the Platform to gather;

(b) the types of information it enters into the Platform for the Customer Request;

(c) the reasons for which it is gathering the information using the Platform;

(d) how the data returned from the Customer Request (Returned Data) will be used by the Customer;

(e) what outcomes the Customer intends to achieve using the Returned Data; and

(f) whether or not the Customer would like to retain the Returned Data and if so, where it would like to store the Returned Data.

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

s. 47(1)(a)

The Department has confirmed that TOR is no longer included in the accounts that are used by the distributed intelligence capability.

s. 47(1)(a)

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

s. 47(1)(a)

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

s. 47(1)(a)

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

Fivecast Onyx

4.31 s. 47(1)(a) Onyx synergises with NexusXplore, providing analysts with the automated ability to comprehensively collect and capture publicly available images and posts against platforms and selectors identified. s. 47(1)(a)

Functional capabilities

s. 47(1)(a)

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

s. 47(1)(a)

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

s. 47(1)(a)

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

4.54 The Department retains full access to audit logs and can review Onyx staff access history and reasons for access by reviewing the audit logs.

OIS

4.55 The Department deploys two specific tools on the OIS environment:

(a) Maltego, which is covered in the original **Open Source Collection Tools PIA dated 11 September 2024**; and

(b) Ripple, which allows for information to be safely and securely moved from the OIS environment to a user's corporate workstation.

4.56 The Department utilises Ecliptic Dynamics' OIS within OGI and provides a virtual machine for more advanced managed attribution compared to Authentic8 Silo, tailoring browser fingerprint and egress location to suit specific requirements.

4.57 OIS is a managed attributed virtual desktop that enables Departmental workers to conduct sensitive advanced online research in a quarantined environment. We understand OIS subscribers to Maltego, like the Department, can access Maltego Enterprise through their OIS account.

s. 47G(1)(a)

4.60 Only authorised and approved Department employees will have access to OIS environment. Access to OIS is only on a departmental issued device or through the departmental network. Department staff can access the departmental network from personal devices when working from home/remotely through the Citrix environment approved by IT. The Citrix environment provides a session hosted on departmental infrastructure so that no work information is stored on personal devices.

Functional capabilities

4.61 The OIS web isolation platform provides a gateway for accessing internet services. Through their cloud server, each OIS user has their own virtual computer which can be accessed securely by a web browser. This virtual computer is rebuilt every 24 hours, and users can browse the internet through this virtual computer. As it is rebuilt daily, any viruses, malware, trackers, online activity and other 'assets' which could become a cyber risk are erased completely. The user's footsteps are also deleted, meaning the user will be almost impossible to track virtually.

4.62 Files from OIS cannot be moved directly to Department infrastructure, creating a further barrier between the user and their online activities through OIS. There is a data storage system entirely separate from OIS which can facilitate data transfer as necessary. Any

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

data leaving that system will be automatically scanned for malware, with any potential threats causing the file to be deleted.

Types of information collected

4.63 Ecliptic Dynamics' privacy policy is more website specific and does not appear to cover the tool. No data appears to be stored by the tool itself. Any data a user wishes to download being first pulled into a separate data storage system before being downloaded locally. The only potential is the storage of sign-in details. Access of the platform is through a web portal, signing in with randomly generated credentials as described above.

Orbis

4.64 ORBIS is a cloud based application, with data extracted through a web user interface.

4.65 We understand the Department has contracted with Moody's (formerly Bureau Van Dijk Electronic Publishing Pty Ltd (BvD)) for their Orbis database. The Department has confirmed that Orbis provides company data on over 400 million businesses and 3-4 billion entities across 190 jurisdictions, resulting in highly consolidated comprehensive datasets considered to be more enhanced and detailed than what other capabilities can provide. ORBIS allows analysts from the Department form connections between individuals and corporate entities that would otherwise be undetectable.

4.66 s. 37(2)(b)

Functional capabilities

4.67 As a cloud based application, Orbis requires users to input search criteria and keywords into their cloud platform.

4.68 Orbis is functionally a powerful data resource on private companies. s. 47(1)(a) ,

s. 47(1)(a)

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

Types of personal information collected:

4.69 While the focus of Orbis is corporate entities, information about key individuals connected with businesses, such as owners, directors, shareholders, managers, professional advisors, and patent holders, in the case of Orbis IP, and information about businesses which are not corporate entities (for example, sole traders) is collected by Orbis.

4.70 According to Orbis' Privacy Policy available at: https://www.moodys.com/web/en/us/legal/privacy-policy.html, Orbis will collect the following personal information to facilitate searches:

(a) name;
(b) contact details (address, email address, telephone number);
(c) gender;
(d) date of birth;
(e) link to LinkedIn profile;
(f) biography;
(g) salary;
(h) education;
(i) disqualification as director;
(j) directorships/roles;
(k) country of resident;
(l) place of birth;
(m) nationality; and
(n) information about unincorporated businesses.

4.71 There is also a specific Privacy Notice for Orbis available at: https://www.moodys.com/web/en/us/legal/orbis-privacy-notice.html.

4.72 Orbis database also provides additional tools that allow for entity resolution and matching of entities based on known criteria.

4.73 The Department is not privy to how Orbis treats, processes, standardises and curates its data in the database. The Department is unable to validate the accuracy of the Orbis database.

4.74 Orbis claims that they run an AI training module to assist with user searches. It is unknown whether user activities and search terms will be automatically captured as part of the AI training module, or if the Department can opt out of the AI training module.

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

Web of Science by Clarivate

4.75 Web of Science is a cloud based application run by Clarivate which provides access to multiple databases that provide reference and citation data from academic journals, conference proceedings, and other documents in various academic disciplines.

4.76 We understand the Department uses Web of Science to perform large scale data analytics of research collaboration between Australian and offshore institutions, in particular to identify academic affiliations or collaborations that may present a threat to Australia's national interest and security.

Functional capabilities

4.77 s. 37(2)(b)

4.78 Data stored in Web of Science is externally hosted by Clarivate on Amazon Web Services with the hosting location of eu-west-1 (Ireland).

4.79 Clarivate has access to delete search history that are associated with a specific user upon request, for example when a user is signed in as a "personalised user". Beyond that Clarivate can only delete search history associated with a particular session. If the user is "anonymous" and not signed in to the application, it is not possible to identify what session to delete.

4.80 Clarivate's privacy policy is available at: https://clarivate.com/privacy-center/notices-policies/privacy-policy/.

4.81 Clarivate Analytics (UK) Ltd is based in the UK, however Clarivate is made up of a number of different legal entities to together form the Clarivate Group. We note it has supplemental privacy notices for:

(a) California;

(b) Virginia, Colorado, Utah and Connecticut;

(c) China under the PIPL; and

(d) Brazil under the LGPD.

Types of information collected:

4.82 Web of Science provides searches to publications and research papers, and therefore limited personal information such as author names may be included in the search results. Personal information may be contained in the publications and research papers as well. Personal information contained in the publications has been collected and published by the authors of publications subject to publishing guidelines.

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

Sayari

4.83 Sayari sources data from over 250 jurisdictions around the globe to fully understand the global supply chain. The Department cross references the information received from Sayari with their own holdings to ensure correctness of the information.

s. 37(2)(b)

4.86 Login credentials for Sayari are maintained by the individuals authorised to use the program.

s. 37(2)(b)

Functional capabilities

s. 47G(1)(a)

Sayari Graph

4.90 Sayari Graph is a commercial risk intelligence platform which fuses global corporate and supply chain data, complex entity networks and intuitive risk identification to assist investigations, intelligence and due diligence.

s. 47G(1)(a)

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

s. 47G(1)(a)

Types of information collected:

4.93 Sayari's Privacy Policy provides how information is collected, and how collected information is used by Sayari. However, the Privacy Policy refers to Sayari customers and does not refer to publicly available personal information collected by the open source collection tool. Sayari's Privacy Policy is available at: https://sayari.com/privacy-policy/.

4.94 Further information on the Data Privacy Framework used by Sayari can be found here: https://www.dataprivacyframework.gov/s/.

4.95 The Department has confirmed information collected by Sayari can include authoritative insight into foreign commercial and trade networks, including information on entities and individuals. We understand Sayari focuses on global corporate and supply chain data, which mainly includes business registration information and corporate information, but may also include personal information such as name, email address and job title of key individuals involved in the supply chain transactions.

4.96 While the focus of Sayari is on fraud, supply chain intelligence, commercial risk intelligence, information collected by Sayari products may also include personal information about key individuals associated with businesses, such as owners, directors, shareholders, managers and professional advisors, individuals transacting with businesses, and information about businesses which are not corporate entities (for example, sole traders).

Benefits of the Project

4.16 The benefits of the project are as stated in **Part 3** of **PIA – Open Source Collection tools dated 1 April 2025.**

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

PART 5: COMPLIANCE WITH THE APPS

OSINT Combine NexusXplore

APP 1 – Open and transparent management of personal information	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. Section 4 of the Privacy Policy provides that the Department 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 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 the assistance of software and ensure all the primary collection purposes have been included in the Privacy Policy (**Recommendation 2**). Recent amendments to the Privacy Act introduced new transparency requirements for businesses and government agencies where: (a) the organisation uses a "computer program" to either: (i) perform decision-making functions in a fully automated manner (without a human decision-maker); or (ii) substantially and directly assist human staff to make decisions; (b) the computer program uses personal information about that individual to perform its function (i.e. to

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

	either make the decision, or to assist the human decision-maker); and (c) the decision could "reasonably be expected to significantly affect the rights or interests of an individual". The term "computer program" is not defined. The explanatory memorandum explains that the new rules are intended to *"encompass a broad range of matters, including pre-programmed rule-based processes, artificial intelligence and machine learning processes"*. OSINT Combine NexusXplore does not use Artificial Intelligence or Machine Learning in the information searching and gathering process, and therefore OSINT Combine is not considered a computer program that assists human decision making. The software is simply streamlining the means by which the Department collects the information, and the information is then assessed and analysed by a human who identifies the relevant material and then draws their own conclusions from that information. Should the functions of OSINT Combine evolve to assist with the analysis and assessment stages, further assessment will be required to determine if the use of OSINT Combine meets the threshold requirement provided in APP 1.7. To prepare for the upcoming Privacy Act changes, we **recommend** the Department include in its Privacy Policy that computer programs are used to assist with intelligence gathering, investigations, research and reporting purposes (**Recommendation 3**).
APP 2 – Anonymity and pseudonymity	**Not Applicable.**
APP 3 – Collection of solicited personal information	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 Departments 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

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

	listed in paragraph 4.5 of the **Open-source Collection Tools PIA**. Any collection, use or disclosure of materials from the 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. When the Department collects information for purposes other than investigations, s 16A exception activities or enforcement related activities, for APP 3.6(b) exception to apply, we have also recommended the Department consider on a case by case basis whether direct collection would jeopardise the purpose of collection resulting in it being unreasonable or impracticable for the Department to collect personal information only from the individual (see **Open Source Collection Tools PIA Recommendation 3**).
APP 4 – Dealing with unsolicited personal information	**Not Applicable.**
APP 5 – Notification of the collection of personal information	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 notifies individuals of collection of their personal information by providing individuals with the Department's general Privacy Notice in Form 1442i, and publishing its Privacy Policy. The OSINT Combine NexusXplore tool constitutes a "contracted service provider" and possibly an "automated system" from whom the Department collects personal information from (**Form 1442i**).As identified in the **Open Source Collection Tools PIA APP 5,** 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. Updates to the Department's Privacy Policy will ensure the individuals are aware of their information being collected and used by the Department. 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

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

	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 paragraph 5.7). 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.
APP 6 – Use or disclosure of personal information	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 of the **Open Source Collection Tools PIA** such as investigation and assessment. 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. 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

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

	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. We **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conduct a research). (**Recommendation 4**) 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. The Department's use of NexusXplore does not constitute a disclosure to the open source collection tools. OSINT Combine has confirmed with the Department that they have zero visibility of the Department's input data, search history or search result, and therefore no personal information is accessible outside of the Department. s. 37(2)(b)
APP 7 – Direct marketing	**Not Applicable.**
APP 8 – Cross-border disclosure of personal information	**Not Applicable.** Based on the analysis above in APP 6, the Department's use of NexusXplore doesn't constitute a disclosure to NexusXplore. There is no cross-border disclosure of personal information by using NexusXplore.

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

APP 9 – Adoption, use or disclosure of government related identifiers	**Not applicable.**
APP 10 – Quality of personal information	The quality of the search results from NexusXplore will be dependent on the accuracy of the NexusXplore database. It is unknown to the Department how NexusXplore maintains its database accuracy. We **recommend** the Department cross reference and verify search results from NexusXplore before relying on it (**Recommendation 6**).
APP 11 – Security of personal information	The NexusXplore platform does not store any data other than the log-in credentials required to access the Platform and the search criteria entered by the Customer unless the persistent monitoring feature of the Platform is utilised by the Customer. Where this feature is utilised, the Platform will store the data from Customer's searches for a period of 12 months. This data can only be accessed by the Customer. Access to use NexusXplore is strictly controlled to Department employees with a business case. Accounts are allocated to individual employees on the basis of a need to use the system within their role. Accounts are all password protected to prevent unauthorised access. OSINT Combine has confirmed with the Department that they have zero visibility of the Department's input data, search history or search result, and therefore no personal information is accessible outside of the Department. Users can technically temporarily record results in the 'Case Management' function of the NexusXplore platform. This is a built-in function of the platform and not a case management or record keeping system of the Department. These 'Cases' are automatically deleted after a period of time. s. 37(2)(b)
APP 12 – Access to personal information	See **Open Source Collection Tools PIA APP 12.**
APP 13 – Correction of personal information	See **Open Source Collection Tools PIA APP 13.**

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

s. 37(2)(b)

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

s. 37(2)(b)

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

s. 37(2)(b)

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

s. 37(2)(b)

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

APP 13 – Correction of personal information	See **Open Source Collection Tools PIA APP 13.**

OIS

APP 1 – Open and transparent management of personal information	OIS is a platform to host other Open Source Collection tools such as Maltego and Ripple. No personal information is collected by OIS directly. Ecliptic Dynamics' privacy policy is more website specific, and does not appear to cover the tool itself. No data appears to be stored by the tool itself, with any data a user wishes to download being first pulled into a separate data storage system before being downloaded locally.
APP 2 – Anonymity and pseudonymity	**Not Applicable**
APP 3 – Collection of solicited personal information	**Not Applicable.** OIS is a managed attributed virtual desktop that enables Departmental workers to conduct sensitive advanced online research in a quarantined environment. No personal information is collected by the OIS tool as it is a working environment for other Open Source Collection Tools.
APP 4 – Dealing with unsolicited personal information	**Not Applicable**
APP 5 – Notification of the collection of personal information	**Not Applicable.**
APP 6 – Use or disclosure of personal information	As mentioned above, we **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conducting a research). (**Recommendation 17**) OIS environment rebuilds itself every 24 hours to clean up historical data to protect user security and privacy. 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.

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

	No personal information will be retained in the OIS environment. OIS environment rebuilds itself every 24 hours to clean up historical data to protect user security and privacy.
APP 7 – Direct marketing	**Not Applicable**
APP 8 – Cross-border disclosure of personal information	**Not Applicable** Based on the analysis above in APP 6, the Department's use of OIS does not constitute a disclosure to OIS. There is no cross-border disclosure of personal information by using the OIS environment.
APP 9 – Adoption, use or disclosure of government related identifiers	**Not Applicable**
APP 10 – Quality of personal information	**Not Applicable**
APP 11 – Security of personal information	s. 37(2)(b)
APP 12 – Access to personal information	See **Open Source Collection Tools PIA APP 12.**
APP 13 – Correction of personal information	See **Open Source Collection Tools PIA APP 13.**

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

Orbis

APP 1 – Open and transparent management of personal information	As mentioned above, we **recommend** the Department include how personal information is collected from online open sources including the assistance of software and ensure all the primary collection purposes of using Orbis have been included in the Privacy Policy (**Recommendation 18**, also see **Open Source Collection Tools PIA Recommendation 2**). Orbis uses Artificial Intelligence in the information searching and gathering process. It is unknown in this Addendum PIA whether user activities and search terms will be automatically captured as part of the AI training module, or if the Department can opt out of the AI training module. We **recommend** the Department understand how AI works in the search process, and incorporating the use of AI in the Department's Privacy Policy (**Recommendation 19**).
APP 2 – Anonymity and pseudonymity	**Not Applicable**
APP 3 – Collection of solicited personal information	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. The Department uses Open Source Collection Tools such as Orbis to conduct investigations for purposes of fulfilling its functions, which includes border management, visa compliance and immigration status resolution, under 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. APP 3.5 provides that an APP entity must collect personal information 'only by lawful and fair means'. We note that open source collection tools may utilise data scraping technologies, and large-scale data scraping may be considered excessive. We have made Recommendation in the **Open Source Collection Tools PIA** and recommend 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 (see **Open Source Collection Tools PIA Recommendation 2**).

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

	When the Department collects information for purposes other than investigations, s 16A exception activities or enforcement related activities, for an APP 3.6(b) exception to apply, we have also recommended the Department consider on a case by case basis whether direct collection would jeopardise the purpose of collection resulting in it being unreasonable or impracticable for the Department to collect personal information only from the individual (see **Open Source Collection Tools PIA Recommendation 3)**.
APP 4 – Dealing with unsolicited personal information	**Not Applicable**
APP 5 – Notification of the collection of personal information	The Department notifies individuals of collection of their personal information by providing individuals with the Department's general Privacy Notice in Form 1442i, and publishing its Privacy Policy. Orbis also outlines what information is being collected and the purposes of information collection in its Privacy Policy and a product specific Privacy Notice. 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 paragraph 5.7). In this Project, notification to individuals will jeopardise the purpose of the collection, for example, when the Department investigates 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.
APP 6 – Use or disclosure of personal information	As mentioned above, we **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conducting a research). **(Recommendation 20)**

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

	Given Orbis is a cloud application, all searches and historical content will be retained in Orbis data platform which allows Orbis staff or authorised third parties used by Orbis as subcontractors to access. s. 37(2)(b) 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. Given Orbis is a cloud application, all searches and historical content will be retained in Orbis data centres, which may be located overseas. We **recommend** the Department identify: (a) the location where information such as search results will be retained; (b) how long the retention period will be; (c) the cloud environment where data will be retained and whether it is a secure environment; (d) from which countries Orbis staff can access data from; (e) for what purposes can Orbis staff access the Department's customer data, and whether Orbis is required to notify the Department; and (f) whether third parties engaged by Orbis may have access to the Department's customer data, and whether Orbis is required to notify the Department. Once the Department has this information, we **recommend** the Department develop operational procedures to minimise the amount of data stored in Orbis and set up internal report storage locations to keep personal information and confidential information in the Department's internal storage in Australia. (**Recommendation 22**)
APP 7 – Direct marketing	**Not Applicable**
APP 8 – Cross-border disclosure of personal information	**Not Applicable**

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

	Based on the analysis above in APP 6, the Department's use of Orbis doesn't constitute a disclosure to Orbis. There is no cross-border disclosure of personal information by using Orbis.
APP 9 – Adoption, use or disclosure of government related identifiers	**Not Applicable**
APP 10 – Quality of personal information	The quality of the search results from Orbis will be dependent on the accuracy of the Orbis database. It is unknown to the Department how Orbis maintains its database accuracy and whether any AI assistance is used by Orbis. We **recommend** the Department cross reference and verify search results from Orbis before relying on it (**Recommendation 23**).
APP 11 – Security of personal information	Orbis is a web based cloud application without any integration to the Department's network. EDW integration with Orbis is outside of the scope for this PIA. s. 37(2)(b) We also **recommend** a further Privacy Impact Assessment be conducted if any integrations were to take place to prevent function creep (e.g. EDW). (**Recommendation 25**)
APP 12 – Access to personal information	See **Open Source Collection Tools PIA APP 12.**
APP 13 – Correction of personal information	See **Open Source Collection Tools PIA APP 13.**

Web of Science

APP 1 – Open and transparent management of personal information	As mentioned above, we **recommend** the Department include how personal information is collected from online open sources including the assistance of software and ensure all the primary collection purposes of using Web of Science have been included in the Privacy Policy

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

	(**Recommendation 26**, also see **Open Source Collection Tools PIA Recommendation 2**). Clarivate states that they use Artificial Intelligence:" *We are fiercely protective of data from all sources to ensure the privacy and security of our customers and partners. Our internal approvals process ensures checks and balances before using generative AI with any of our products or services, or before allowing any third party to use our content and products within their use of generative AI.*" We **recommend** the Department understand how AI works in the search process and incorporating the use of AI in the Department's Privacy Policy (**Recommendation 27**).
APP 2 – Anonymity and pseudonymity	**Not Applicable.**
APP 3 – Collection of solicited personal information	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. The Department uses Open Source Collection Tools such as Web of Science to conduct investigations for purposes of fulfilling its functions, which includes 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 is required to collect personal information only from the individual under APP 3.6. Given Web of Science deals with publications and research papers, limited personal information such as author names may be included in the search results. Limited personal information may be contained in the publications and research papers as well. Personal information contained in the publications has been collected and published by the authors of publications subject to publishing guidelines. It is impractical for the Department to collect consent from each individual when their personal information has already been made public by the authors of the research papers (APP 3.6(b)). Therefore the Department is not required to collect consent from individuals when collecting their personal information referred to in the publications and research papers. According to APP 3.3, the Department must not collect sensitive information unless explicit consent has been

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

	provided by the individual, or if an exception under 3.4 applies. It is generally not expected for any research papers to contain sensitive information as publishing guidelines often strictly require removal of sensitive information before making such information publicly available. In the unlikely event for publications or research papers to contain sensitive information, the Department can be exempted from the consent collection if the Department is collecting this information for a court or tribunal order, enforcement related activities or one of permitted general situations under s 16A of the Privacy Act subject to APP 3.4. If none of the APP 3.4 exception applies, the Department will need to check if the publications or research papers contains consent declaration by the individual, or else the Department will be required to collect consent from the individual before such sensitive information can be collected and used by the Department. Based on the analysis above, considering publications and research papers generally do not contain sensitive information according to Clarivate's Privacy Policy, we consider the use of Web of Science compliant with APP 3.
APP 4 – Dealing with unsolicited personal information	**Not Applicable.**
APP 5 – Notification of the collection of personal information	The Department notifies individuals of collection of their personal information by providing individuals with the Department's general Privacy Notice in Form 1442i, and publishing its Privacy Policy. Web of Science's provider Clarivate also outlines what information is being collected and the purposes of information collection in its Privacy Policy. 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 paragraph 5.7). For this Project, notification to individuals would 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

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

	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.
APP 6 – Use or disclosure of personal information	As mentioned above, we **recommend** the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conducting a research). **(Recommendation 28)** Given Web of Science is a cloud application, all searches and historical content will be retained in Clarivate data centre located in Ireland. It will also allow Clarivate staff or authorised third parties used by Clarivate as subcontractors to access. Clarivate has confirmed that search history can be deleted upon request if the person performing searches is logged into their user account. s. 37(2)(b)
APP 7 – Direct marketing	**Not Applicable.**
APP 8 – Cross-border disclosure of personal information	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, and therefore does not constitute as an overseas disclosure under APP 8. s. 37(2)(b)

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

s. 37(2)(b)

APP 9 – Adoption, use or disclosure of government related identifiers	**Not Applicable**
APP 10 – Quality of personal information	The quality of the search results from Web of Science will be dependent on the accuracy of the Web of Science database. It is unknown to the Department how Clarivate maintains its database accuracy and whether any AI assistance is used by Orbis. We **recommend** the Department cross reference and verify search results from Web of Science before relying on it (**Recommendation 30**).
APP 11 – Security of personal information	Web of Science is a web based cloud application without any integration to the Department's network. Given search results may contain personal information and sensitive information, we **recommend** the Department store such information in a secure location on the Department's internal servers (**Recommendation 31**). Given function restrictions in place, we **recommend** the Department always log in as a 'Personalised User' for audit and tracking purposes (**Recommendation 32**).
APP 12 – Access to personal information	See **Open Source Collection Tools PIA APP 12.**
APP 13 – Correction of personal information	See **Open Source Collection Tools PIA APP 13.**

s. 37(2)(b)

Sayari

APP 1 – Open and transparent management of personal information	As mentioned above, we **recommend** the Department include how personal information is collected via Sayari and ensure all the primary collection purposes of using Sayari have been included in the Privacy Policy (**Recommendation 34**, also see **Open Source Collection Tools PIA Recommendation 2**).

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

	Sayari Map uses AI in the process of supplier mapping and risk screening to identify trade relationships. It is unknown in this Addendum PIA how this AI component functions, if any user activities are captured as part of the AI training, or if the Department can opt out of the AI training module. We recommend the Department understand how AI functions in Sayari impact the search process, and incorporating the use of AI in the Department's Privacy Policy (**Recommendation 35**).
APP 2 – Anonymity and pseudonymity	**Not Applicable.**
APP 3 – Collection of solicited personal information	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. The Department uses Open Source Collection Tools such as Sayari to conduct investigations for purposes of fulfilling its functions, which includes 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. When the Department collects information for purposes other than investigations, s 16A exception activities or enforcement related activities, for an APP 3.6(b) exception to apply, we have also recommended the Department consider on a case by case basis whether direct collection would jeopardise the purpose of collection resulting in it being unreasonable or impracticable for the Department to collect personal information only from the individual (see **Open Source Collection Tools PIA Recommendation 3)**.
APP 4 – Dealing with unsolicited personal information	**Not Applicable.**
APP 5 – Notification of the collection of personal information	The Department notifies individuals of collection of their personal information by providing individuals with the Department's general Privacy Notice in Form 1442i, and publishing its Privacy Policy. Sayari also outlines what information is being collected and the purposes of information collection in its Privacy Policy. 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

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

	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 paragraph 5.7). The Department should be mindful to avoid using open source collection tools where information is collected from websites where consent has not been provided (e.g. from data scraping). A good practice for the Department is to review the privacy policy provided by the service provider and see if their privacy policy lists all the relevant information required under APP 1.4 and complies with the OAIC's requirements outlined in the What is a privacy policy? | OAIC. 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.
APP 6 – Use or disclosure of personal information	As mentioned above, we recommend the Department ensure the secondary use and disclosure purpose falls within one of the exceptions outlined in APP 6.2 or de-identify any personal information that is not relevant to the primary purpose of the Project (e.g. preparing a report or conducting a research). (**Recommendation 36**) Search results will be stored in appropriate Departmental databases, such as NIS. The Department has confirmed that all search results will be stored within the Department and will not be accessible to any third parties, including to Sayari staff. 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.

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

	The Department's use of Sayari does not constitute a disclosure to Sayari.
APP 7 – Direct marketing	**Not Applicable.**
APP 8 – Cross-border disclosure of personal information	**Not Applicable.** Based on the analysis above in APP 6, the Department's use of Sayari doesn't constitute a disclosure to Sayari. There is no cross-border disclosure of personal information by using Sayari.
APP 9 – Adoption, use or disclosure of government related identifiers	**Not Applicable.**
APP 10 – Quality of personal information	The quality of the search results from Sayari will be dependent on the accuracy of the Sayari database. It is unknown to the Department how Sayari maintains its database accuracy. Sayari has confirmed that AI assistance is used to generate data mapping. However, the details of how the enablement of AI improves the quality of the search results is not disclosed by Sayari. We recommend the Department cross reference and verify search results from Sayari before relying on it (**Recommendation 37**).
APP 11 – Security of personal information	Sayari products are installed on the Department's internal environment. Search results from Sayari products will be stored in appropriate Departmental databases, such as National Intelligence System (NIS). All internal storage databases are governed by Whole of Government data retention policies and legislation. Login credentials for Sayari are maintained by the individuals authorised to use the program. We are satisfied that the use of Sayari complies with APP 11 requirements.
APP 12 – Access to personal information	See **Open Source Collection Tools PIA APP 12.**
APP 13 – Correction of personal information	See **Open Source Collection Tools PIA APP 13.**

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

PART 6: PRIVACY IMPACT ANALYSIS AND COMPLIANCE CHECK

6.1 The OAIC 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?

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

Additional compliance questions

6.3 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?

6.4 When providing information to the Department, individuals do surrender control of that information to some extent. However, 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.

6.5 Further, individuals are made aware of the potential use and disclosure of their personal information, including for description, via Form 1442i, and in the Department's Privacy Policy on its website.

6.6 We have made relevant recommendations to update the Department's Privacy Policy to better clarify how the Department uses the Open Source Collection Tools.

6.7 In light of recent amendments to the Privacy Act, we have also recommended the department to include in its Privacy Policy whether a computer program is used to perform decision-making functions in a fully automated manner (without a human decision-maker) or to substantially and directly assist human staff to make decisions.

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?

6.8 No, the Project does not change how individuals interact with the Department.

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)?

6.9 The Department may make various decisions based on the findings from Open Source Collection Tools. Such decisions are consistent with the Department's current functions.

6.10 We have made recommendations to the Department to ensure accuracy and quality of the information has been validated before relying on such information to make a decision.

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

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

6.11 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.

6.12 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?

6.13 Privacy breaches are managed in accordance with the Department's existing Privacy breaches and Notifiable Data Breaches Scheme document.

6.14 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 38**).

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

6.15 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).

6.16 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.

6.17 We **recommend** the Department regularly conduct security audit and third party security assessments on the Open Source Collection Tools in case of updates and new functions and features being added to the tools (**Recommendation 39**).

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?)

6.18 There is a risk of "function creep" where there is an expansion in the purposes for which personal information associated with the Project is used or disclosed (that is, for secondary purposes not initially anticipated). We **recommend** the Department implement processes and governance arrangements to ensure function creep does not occur, such as periodic reviews that information collected in respect of the Project continues to be used by the Department solely for the primary purpose of collection (**Recommendation 40**).

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

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?)

6.19 The information would be highly valuable to unauthorised users as it contains key identity information and sensitive information of a vulnerable group of individuals.

6.20 We have made recommendations to the Department to have 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?

6.21 The Project uses information already collected by the Department and therefore does not imply an increase in invasiveness.

6.22 As a privacy-positive strategy, we **recommend** a post-implementation audit six months 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 41**).

How consistent is the project with community values about privacy?

6.23 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'.

6.24 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.'

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

griffinlegal.

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	*Privacy (Australian Government Agencies – Governance) APP Code 2017*. 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 *Privacy Act 1988*.
APP Guidelines	The OAIC's publication *Australian Privacy Principles Guidelines*, available at Australian Privacy Principles guidelines | OAIC
Archives Act	*Archives Act 1983* (Cth)
CRM	Customer Relationship Management
Department	Department of Home Affairs
DNS	Domain Name System
EDW	Enterprise Data Warehouse
EULA	End User Licence Agreement
Intelligence capability	The Department's dispersed intelligence teams formerly contained in the Intelligence Division
IP	Internet Protocol
FOI Act	*Freedom of Information Act 1982* (Cth)
GL	Griffin Legal
GPT	Generative Pre-training Transformer
Health Information Section 6FA, *Privacy Act*	(a) information or an opinion about: (i) the health, including an illness, disability or injury, (at any time) of an individual; or

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

	(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; 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.
ISM	Information Security Manual
IoT	Internet of Things
NIS	National Intelligence System.
OSINT	Open Source Intelligence
OGI	Online and Geospatial Intelligence Section
OAIC	Office of the Australian Information Commissioner
OAIC 2020 survey	The OAIC's publication *Australian Community Attitudes to Privacy Survey 2020*, available at Australian Community Attitudes to Privacy Survey 2020 | OAIC
OAIC 2023 survey	The OAIC's publication *Australian Community Attitudes to Privacy Survey 2023*, available at Australian Community Attitudes to Privacy Survey 2023 | OAIC
OIS	OIS is a web isolation platform developed by Eclipse Dynamics See OIS - Web Isolation Platform | Ecliptic Dynamics for more details.
Personal Information, Section 6, *Privacy Act*	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), *Privacy Act*	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

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

	(b) sets out recommendations for managing, minimising or eliminating that impact.
PIA Guide	The OAIC's publication *Guide to undertaking privacy impact* assessments, available at: Guide to undertaking privacy impact assessments | OAIC
Privacy Act	*Privacy Act 1988* (Cth)
Privacy Policy	The Department's Privacy Policy, available at Privacy (homeaffairs.gov.au)
Project	Open-Source Collection Tools
PSPF	Protective Security Policy Framework
SRA	Security Risk Assessment
Sensitive Information – Section 6, *Privacy Act*	(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.

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