

Document 1 (pages 1-7) deleted under section 42(1) of the ***Freedom of Information Act 1982*** (Cth).



Threshold Assessment

Fivecast ONYX

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

Project or initiative

Brief project or initiative description and intended goals/outcomes	Intelligence and Fraud investigations teams within the Department of Employment and Workplace Relations (the department) require multiple sources of information to derive quality insights and link suspicious activity. Leveraging Open-Source data, the Fivecast ONYX product enables users to access this information in a single, secure environment.
Key implementation date/s	July 2023
Key internal and external stakeholders	Compliance Intelligence Team Skills Compliance Delivery Team Enterprise Risk, Assurance and Investigations (Fraud) Platform Design and Architecture Team Fivecast (external)

Section 1: Personal information

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

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

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



Australian Government
**Department of Education,
 Skills and Employment**

Email addresses	☒	☒	☐	☒	☐	☐
Telephone numbers	☒	☒	☐	☒	☐	☐
Dates of birth	☒	☒	☐	☒	☐	☐
Sex or gender	☒	☒	☐	☒	☐	☐
Opinions or feedback	☒	☒	☐	☒	☐	☐
Commentary	☐	☐	☐	☐	☐	☐
CRNs or JSIDs	☐	☐	☐	☐	☐	☐
USIs or CHESSNs	☐	☐	☐	☐	☐	☐
Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☐	☐	☐	☐	☐	☐
Bank account details	☐	☐	☐	☐	☐	☐
Identity documents	☐	☐	☐	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☐	☐	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
Social Media posts such as business marketing and advertising and other information individuals have posted on their social media accounts. The information, including opinions is limited to what has been posted publicly. Fivecast will require staff usernames and email addresses to create an account. Departmental email addresses will be used in place of personal email addresses. It is anticipated that for 12-months there will be individual licences for 5 departmental staff to access Fivecast. This will be revisited in future prior to extending licensing arrangements.						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative? <i>You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.</i>						



The information will be used by the authorised staff in relevant compliance and intelligence teams and access managed by the Compliance Intelligence team. How many staff will be authorised to have access will be determined on an as required and appropriate basis. The tool will be used to help establish relationships between entities/organisations as part of compliance activities³ and to support any ongoing investigations. The information derived from the software will be used for intelligence purposes to understand aspects of a business or individual associated with the business and whether this poses a risk to the eligibility to, or payment integrity of, a program or programs. The information will be viewed by authorised departmental staff and where relevant will be recorded and secured in an appropriate DEWR case management environment (such as SID).

All information that is identified by the software can already be found on social media in a public setting and is available to any member of the public, including those outside of the department. The software provides an efficient means to collect information from multiple social media platforms without storing immediately within DEWR environment (web-based tool), flagging DEWR interests in parties or known sharp practices and establishes effective linkages (via APIs and tradecraft) that are not easily replicated on a large scale by general users of the public.

The information consolidated by Fivecast is collected from third party social media sites. These social media companies may store this information on cloud or other data centres globally. Fivecast stores its information on Australian-hosted servers and satisfies all current Commonwealth security requirements. This is evidenced through its use with other Commonwealth departments, including security agencies.

The department is not directly involved in the collection or storage of the public information and is an end user of the product. Only when information is relevant to intelligence and compliance activities will the discrete data sets be downloaded from the web-based tool into the department's environment. In these circumstances, the relevant information would be extracted into excel or chart form and saved in the department's internal IT environment.

The information viewed in Fivecast is used to inform lines of inquiry, to establish intelligence links and is not used as evidence. Where information is relevant to an investigation, it will be second-sourced and that second-sourced information (not information directly from Fivecast) may then potentially be relied upon as evidence and disclosed externally.

How many individuals' personal or sensitive information will be handled in the project or initiative?	100 – 1000 annually
---	---------------------

³ Compliance means conforming to a relevant rule, such as a specification, policy, regulation, standard or law.

A compliance breach occurs when there is a failure to comply with a legislative obligation, that may be established in Rules, Policies, Procedures or Guidelines.

Breaches can occur, for example, through human error, technical issues, misinterpretation of the obligations, or through a deliberate act.

A compliance activity is an activity that will attempt to identify and resolve a relevant compliance breach.

This may include raising of a debt, issuing a infringement notice, education, notification to DEWR Fraud Team or relevant external agency.



Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way? If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.	No
☐ The <u>nature or type</u> of the personal information being handled is new or different.	
☐ The <u>scope</u> of the personal information being handled is new or different.	
☐ The personal information is being handled in a new or different <u>context</u>.	
☐ The <u>purpose</u> for which the personal information is being handled is new or different.	
☐ The <u>risk</u> of handling the personal information is new or different.	
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
Fivecast has been used by the department previously. However, this PTA is being completed as best practice.	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s). You should provide the name of the same or similar project or initiative <u>where the practice(s) have been assessed previously</u> and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	
Fivecast is considered a well-established and highly regarded web-based software by the Commonwealth government and within the National Intelligence Community. The software has been effectively deployed across a range of Australian and International agencies and Departments, with successful development and trailing previously undertaken by DESE (prior to MOG changes) and the Department of Education (Education). The software is currently being used by DEWRs Commonwealth partners (s 22(1)) and until recently was available within the Department (until January 2023 where licensing arrangements expired). There is currently an appetite within the Department to revisit the licensing arrangements and engage this software vendor once again. In the absence of Fivecast (or a dedicated OSINT solution), Departmental staff must manually search a broad range of social media sites for any results matching entities of interest. Without however the authentication of user credentials and an inability for staff to create 'false' accounts, access to information on many social media sites is severely limited or withheld until a staff member can log in. The use of Fivecast allows a user to search across these multiple platforms simultaneously without requiring the creation of log in details (managed pools via Fivecast) and without overtly exposing the Department's interest in entities to third party companies.	



The use of FiveCast simply provides a platform for this information in a consolidated place for a more efficient and safe way to access it with no direct engagement with social media platforms themselves.

The Skills Programs Compliance Branch has existing privacy and security processes and procedure around the collection and storage of personal information for reporting purposes, compliance and intelligence activities. The collection of this information will not be treated differently to personal data already collected.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?	No
To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	
☐ Handling large amounts of personal information.	
☒ Handling sensitive information ⁴ .	
☐ Handling personal information in a way that is likely to raise public concern or unlikely to have community support.	
☒ Handling the personal information of individuals who are vulnerable. ⁵	
☒ Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.	
☐ Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.	
☐ Using or disclosing personal information for profiling or behavioural predictions.	
☐ Using personal information for automated decision-making.	
☐ Collecting personal information through systematic monitoring or tracking of individuals.	
☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.	
☒ Using information for data matching or linking unconnected personal information.	
☐ Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.	
☒ Handling personal information for activities of a long term or permanent duration.	
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	

⁴ Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

⁵ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.



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

The information collected is data that has been made available for public use. The terms and conditions, including options to not post the information for public consumption is handled separately by each of the social media sites themselves, with the content only made publicly available on these platforms once this consent has been obtained from the member of the public.

All information considered relevant to the Department's compliance and investigation activities (our purposes) identified using the Fivecast platform, and extracted for our purposes will be treated in accordance with existing privacy and security framework, including the information handling and security procedures currently in place. If at any point the information identified is deemed no longer relevant for these purposes then the information will be removed. If there are any changes identified after this assessment has been undertaken that could have an impact on privacy considerations, then a new threshold assessment will be undertaken.

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

Yes

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

Outcome

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

Outcome

A PIA is not required as there are no high privacy risk elements or no new or changed ways of handling personal information

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

Approved by **s 22(1)**

Date: 25/07/2023

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



Australian Government
**Department of Education,
Skills and Employment**



Threshold Assessment

Fivecast ONYX

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

Project or initiative

Brief project or initiative description and intended goals/outcomes	Intelligence and Fraud investigations teams within the Department of Employment and Workplace Relations (the department) require multiple sources of information to derive quality insights and link suspicious activity. Leveraging Open-Source data, the Fivecast ONYX product enables users to access this information in a single, secure environment.
Key implementation date/s	July 2023
Key internal and external stakeholders	Compliance Intelligence Team Skills Compliance Delivery Team Enterprise Risk, Assurance and Investigations (Fraud) Platform Design and Architecture Team Fivecast (external)

Section 1: Personal information

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

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

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



Australian Government
**Department of Education,
 Skills and Employment**

Email addresses	☒	☒	☐	☒	☐	☐
Telephone numbers	☒	☒	☐	☒	☐	☐
Dates of birth	☒	☒	☐	☒	☐	☐
Sex or gender	☒	☒	☐	☒	☐	☐
Opinions or feedback	☒	☒	☐	☒	☐	☐
Commentary	☐	☐	☐	☐	☐	☐
CRNs or JSIDs	☐	☐	☐	☐	☐	☐
USIs or CHESSNs	☐	☐	☐	☐	☐	☐
Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☐	☐	☐	☐	☐	☐
Bank account details	☐	☐	☐	☐	☐	☐
Identity documents	☐	☐	☐	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☐	☐	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
Social Media posts such as business marketing and advertising and other information individuals have posted on their social media accounts. The information, including opinions is limited to what has been posted publicly. Fivecast will require staff usernames and email addresses to create an account. Departmental email addresses will be used in place of personal email addresses. It is anticipated that for 12-months there will be individual licences for 5 departmental staff to access Fivecast. This will be revisited in prior to extending licensing arrangements.						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative? <i>You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.</i>						



The Fivecast software provides an efficient means to collect information from multiple social media platforms without storing immediately within DEWR environment, flagging DEWR interests in parties or known sharp practices and establishes effective linkages (via APIs and tradecraft) that are not easily replicated on a large scale by general users of the public.

All information that is identified by the Fivecast software is existing information found on social media. It is public and available to any member of the public. The information is collected and consolidated by Fivecast from third party social media sites. These social media companies may store this information on cloud or other data centres globally.

Fivecast is a web-based tool and stores its information on Australian-hosted servers and satisfies all current Commonwealth security requirements. This is evidenced through its use with other Commonwealth departments, including security agencies. The department is not directly involved in the collection, consolidation or storage of the public information and is an end user of the product.

The tool will be used to help establish relationships between entities/organisations as part of assurance and compliance activities³ and to support any ongoing investigations. The information derived from the software will be used for intelligence, assurance and compliance purposes to understand aspects of a business, or individual associated with the business, and whether this poses a risk to the eligibility to, or payment integrity of, a program or programs.

Only when information is relevant to intelligence, assurance and compliance activities will the discrete data sets be downloaded from Fivecast into the department's environment. In these circumstances, the relevant information would be extracted into excel or chart form and saved, and secured appropriately, in the department's internal IT environment.

As noted above, the information viewed in Fivecast is used to inform lines of inquiry, to establish intelligence links and is not used as evidence. Where information is relevant to an investigation, it will be second-sourced and that second-sourced information (not information directly from Fivecast) may then be relied upon as evidence and disclosed externally.

The information will be used by the authorised staff in the relevant compliance and intelligence teams. Access will be managed by the Compliance Intelligence team. The number of staff authorised to have access will be determined on an as required and appropriate basis.

³ Compliance means conforming to a relevant rule, such as a specification, policy, regulation, standard or law.

A compliance breach occurs when there is a failure to comply with a legislative obligation, that may be established in Rules, Policies, Procedures or Guidelines.

Breaches can occur, for example, through human error, technical issues, misinterpretation of the obligations, or through a deliberate act.

A compliance activity is an activity that will attempt to identify and resolve a relevant compliance breach.

This may include raising of a debt, issuing a infringement notice, education, notification to DEWR Fraud Team or relevant external agency.



The information will be viewed by authorised departmental staff and where relevant will be recorded and secured in an appropriate DEWR case management environment (such as SID).

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

100 – 1000
 annually

Section 2: New or changed ways of handling personal information

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

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

No

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

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

Fivecast has been used by the department previously. However, this PTA is being completed as best practice.

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

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

Fivecast is considered a well-established and highly regarded web-based software by the Commonwealth government and within the National Intelligence Community.

The software has been effectively deployed across a range of Australian and International agencies and Departments, with successful development and trailing previously undertaken by DESE (prior to MOG changes) and the Department of Education (Education).

The software is currently being used by DEWRs Commonwealth partners (s 22(1)) and until recently was available within the Department (up to January 2023 where licensing arrangements expired). There is an appetite within the Department to revisit the licensing arrangements and use the software.

In the absence of Fivecast (or a dedicated OSINT solution), Departmental staff manually search a broad range of social media sites for any results matching entities of interest. Without however



the authentication of user credentials and an inability for staff to create 'false' accounts, access to information on many social media sites is severely limited or withheld until a staff member can log in.

The use of Fivecast allows a user to search across these multiple platforms simultaneously without requiring the creation of log in details (managed pools via Fivecast) and without overtly exposing the Department's interest in entities to third party companies. It provides a platform for this information to be consolidated more efficient and a safe way to access it with no direct engagement with social media platforms themselves.

The Skills Programs Compliance Branch has existing privacy and security processes and procedure around the collection and storage of personal information for reporting purposes, assurance, compliance and intelligence activities. The collection of this information will not be treated differently to personal data already collected.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals? To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	No
☐ Handling large amounts of personal information. ☒ Handling sensitive information⁴. ☐ Handling personal information in a way that is likely to raise public concern or unlikely to have community support. ☒ Handling the personal information of individuals who are vulnerable.⁵ ☒ Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft. ☐ Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers. ☐ Using or disclosing personal information for profiling or behavioural predictions. ☐ Using personal information for automated decision-making. ☐ Collecting personal information through systematic monitoring or tracking of individuals. ☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.	

⁴ Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

⁵ May include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.



Australian Government
**Department of Education,
 Skills and Employment**

☒	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
The information collected is data that has been made publicly available by the entity or individual. The terms and conditions, including options to not post the information for public consumption is handled separately by each of the social media sites themselves, with the content only made publicly available on these platforms once consent has been obtained from the member of the public. All information considered relevant to the Department's assurance, compliance and investigation activities (our purposes) identified using the Fivecast platform, and extracted for our purposes will be treated in accordance with existing privacy and security framework, including the information handling and security procedures currently in place. If at any point the information identified is deemed no longer relevant for these purposes then the information will be removed. If there are any changes identified after this assessment has been undertaken that could have an impact on privacy considerations, then a new threshold assessment will be undertaken.	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Outcome

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

Outcome	A PIA is not required as there are no high privacy risk elements or no new or changed ways of handling personal information
---------	---



Australian Government
**Department of Education,
Skills and Employment**

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

Approved by: s 22(1)

Assistant Secretary, Skills Programs Compliance Branch

s 22(1)

Date: 26/07/2023

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

S 22(1)

From S 22(1) <S 22(1)@dewr.gov.au>
Sent: Tuesday, July 25, 2023 3:28 PM
To: S 22(1) <S 22(1)@dewr.gov.au>

Cc: DEWR - Compliance Intelligence <S 22(1) @dewr.gov.au>; S 22(1)
<S 22(1) @dewr.gov.au>; S 22(1) <S 22(1) @dewr.gov.au>; S 22(1)
S 22(1) @dewr.gov.au>

<s 22(1)

Subject: Request for AS Approval - Fivecast ONYX PTA (Updated) S 22(1)

Importance: High

S 22(1)

Good Afternoon S 22(1),

I am seeking your approval for an updated Privacy Threshold Assessment (PTA) for Fivecast ONYX (first attachment).

This PTA seeks to enable the use of the Fivecast ONYX SaaS for Skills Programs Compliance purposes under the Enhancing Operational Intelligence across Skills Programs (EOISP) project. It will also provide broader capability for the Corporate Fraud team, who have also expressed a need for using the software (and recently onboarded a trained user). This is also considered an enhancement to the Intelligence Capability of DEWR and will support the Intel 'Beneficial Ownership' project. This includes potential identification of undeclared conflicts of interest through undeclared relationships, business affiliations and broader links to entities.

S 22(1)

s 22(1)

Director

Compliance Intelligence | Skills Program Compliance Branch
VET Data, Loans and Compliance Division
Australian Government Department of Employment and Workplace Relations (DEWR)
Phone S 22(1) | Mobile S 22(1)
dewr.gov.au

The Department of Employment and Workplace Relations acknowledges the traditional owners and custodians of country throughout Australia and their continuing connection to community. We pay our respects to them and their cultures, and Elders past, present and emerging.

s 22(1)

s 22(1)

From: s 22(1) s
Sent: Thursday, 28 September 2023 10:19 AM
To: s 22(1)
Cc: s 22(1) s 22(1) (EAN) s 22(1) s 22(1)
Subject: RE: Fivecast sourcing business case [SEC=OFFICIAL]

Good morning s 22(1)

s 22(1) has pointed us in your direction for further work with the Fivecast business case. I've had a look and adjusted some of it, though as the business case uses a lot of our wording from the Fivecast PTA it was already very consistent with our framing.

Feel free to reach out if any clarification or discussion is required.

Business Case

The Enhancing Operational Intelligence across Skills Programs 2023-24 DCB funded project undertaken by the Skills Programs Compliance Branch aims to uplift intelligence capability for the Department's compliance delivery of Australian Government funded skills programs. One component of this project is procuring Fivecast ONYX (Fivecast). Fivecast is a SaaS product that provides Compliance and Intelligence officers with the ability to identify undeclared relationships, business affiliations and broader links to entities that the department needs to utilise in its reviews and investigations, among other compliance and fraud detection capabilities.

Fivecast ONYX is a proprietary solution used by numerous Government entities to perform targeted analysis on a unique range of platforms across the surface, deep, and dark web to resolve identities. The Compliance Intelligence team will use this data to search a broad range of platforms for insights about current and potential providers. Without this tool Departmental staff have to manually search a broad range of social media sites for any results matching entities of interest, which is limited to what can be sourced on the surface web and further limited by access requirements of these sites. The use of Fivecast allows a user to search across these multiple platforms simultaneously without requiring the creation of log in details and without overtly exposing the Department's interest in entities to third party companies. It provides a platform for this information to be consolidated in a more efficient and safe way, with no direct engagement with social media platforms themselves. The in-depth functionality and unique analytical expertise and tradecraft offered by Fivecast saves considerable departmental effort and provides superior outcomes, minimising the financial, policy and reputational risks of dealing with high-risk providers. It also allows for these searches to be performed in a consistent, repeatable manner and provides persistent insights which are essential to the Compliance Intelligence team's risk assessment framework.

Fivecast has been used in the department since 2019, but in January 2023 the contract was allowed to lapse while the newly formed Compliance Intelligence team still had an ongoing use case for the product. This process is to re-procure this product to satisfy this ongoing departmental requirement.

Market research question

Fivecast is the only supplier who delivers this specialised product capable of providing potential identification of undeclared relationships, business affiliations, and broader links to entities that the department needs to utilise for effective investigations. Fivecast ONYX uses one of a kind proprietary data collection technology to enable analysts to perform searches and serve insights with unique knowledge and usage in the Australian Intelligence Community. This product is unique in terms of the manner in which the data is sourced, the range of sources, including sources below surface level internet, and the compilation and insight provided.

As there are no alternate software products available with the same functional capability that are compliant with Australian Government HCF and cyber requirements, a limited tender will be used in compliance with 10.3 d. iii) of the CPRs. Fivecast has previously been procured by DEWR/Department of Education under CPR 10.3 both in 2019

and again in 2022 and is considered the value for money by reason of the lack of alternatives and the costs saved in the department by using this product. Fivecast ONYX is available via the DTA Software and Licencing Services Panel and can be procured via limited tender from that panel.

Cheers,
S 22(1)
Senior Intelligence Analyst
Compliance Intelligence | Skills Programs Compliance
VET Data, Loans and Compliance Division
Australian Government Department of Employment and Workplace Relations
Phone S 22(1) | Ext. S 22(1)
www.dewr.gov.au

The Department of Employment and Workplace Relations acknowledges the traditional owners and custodians of country throughout Australia and their continuing connection to land, waters and community. We pay our respects to them and their cultures, and Elders past, present and emerging.

S 22(1)

S 22(1)

S 22(1)

From: S 22(1)
Sent: Thursday, September 21, 2023 10:44 AM
To: S 22(1) I <S 22(1) [@dewr.gov.au](mailto:S 22(1)@dewr.gov.au)>
Cc: TS 22(1) <S 22(1) [@dewr.gov.au](mailto:S 22(1)@dewr.gov.au)>; S 22(1) S 22(1) [@dewr.gov.au](mailto:S 22(1)@dewr.gov.au);
S 22(1) <S 22(1) [@dewr.gov.au](mailto:S 22(1)@dewr.gov.au)>
Subject: Fivecast sourcing business case

Good morning S 22(1)

s 22(1)

I had a quick first go at a business case for Fivecast. Do you mind please reviewing, making any changes (I'm still getting familiar with things so guarantee there will be some bits that don't fit the reality of your use case) and adding in any additional context you think might be persuasive?

There will be two elements the business case itself for the product, and the case for a limited tender:

Business Case

The Skills Group Enhancing Operational Intelligence across Skills Program 2023-24 DCB funded project aims to uplift compliance capability for the Department's delivery of Australian Government funded skills programs. One component of this project is procuring Fivecast Onyx (Fivecast). Fivecast is a SaaS product that provides Skills Program Compliance Intelligence officers with the ability to identify undeclared relationships, business affiliations and broader links to entities that the department needs to utilise in its investigations, among other compliance and fraud detection capabilities.

Fivecast Onyx is a proprietary solution used by numerous Government entities to perform targeted analysis on a unique range of platforms across the surface, deep, and dark web data to resolve identities. The Compliance Intelligence team use this data to search a broad range of platforms for insights about current and potential providers. Without this tool Departmental staff have to manually search a broad range of social media sites for any results matching entities of interest, but this is limited to what can be sourced on the surface web and further limited by access requirements of these sites. The use of Fivecast allows a user to search across these multiple platforms simultaneously without requiring the creation of log in details and without overtly exposing the Department's interest in entities to third party companies. It provides a platform for this information to be consolidated in a more efficient and safe way, with no direct engagement with social media platforms themselves. The in-depth functionality and unique analytical expertise and tradecraft offered by Fivecast saves considerable departmental effort and provides superior outcomes,⁹⁶ minimising the financial, policy and reputational risks of dealing with high-risk providers. It also allows for these searches to be performed in a consistent, repeatable manner and provides persistent insights which are essential to the Compliance Intelligence team's risk assessment framework.

Fivecast has been used in the department since 2019, but in January 2023 the contract was allowed to lapse while the newly formed the Compliance Intelligence team still had an ongoing use case for the product. This process is to re-procure this product to satisfy this ongoing departmental requirement.

Market research question

Fivecast is the only supplier who delivers this specialised product capable of providing potential identification of undeclared relationships, business affiliations, and broader links to entities that the department needs to utilise for effective investigations. Fivecast Onyx uses one of a kind proprietary data collection technology to enable analysts to perform searches and serve insights with unique knowledge and usage in the Australian Intelligence Community. This product is unique in terms of the manner in which the data is sourced, the range of sources, including sources below surface level internet, and the compilation and insight provided.

As there are no alternate software products available with the same functional capability that are compliant with Australian Government HCF and cyber requirements, a limited tender will be used in compliance with 10.3 d. iii) of the CPRs. Fivecast has previously been procured by DEWR/Department of Education under CPR 10.3 both in 2019 and again in 2022 and is considered the value for money by reason of the lack of alternatives and the costs saved in the department by using this product. Fivecast Onyx is available via the DTA Software and Licencing Services Panel and can be procured via limited tender from that panel.

s 22(1)

Kindest Regards

s 22(1)

Assistant Director

Data Analytics Platforms and Warehousing | Data Platforms and Education Systems

Digital Solutions Division

Australian Government Department of Employment and Workplace Relations

Phone S 22(1)

dewr.gov.au

The Department of Employment and Workplace Relations acknowledges the traditional owners and custodians of country throughout Australia and their continuing connection to community. We pay our respects to them and their cultures, and Elders past, present and emerging.

s 22(1)

From: s 22(1)
Sent: Monday, 9 September 2024 11:34 AM
To: s 22(1)
Subject: Fivecast Onyx Subscription-Renewal due 30/11/2024 [SEC=OFFICIAL]
Attachments: ICTSR-23-2536.pdf

Follow Up Flag: Follow up
Flag Status: Completed

Categories: EOISP, Important, Admin

Hi s 22(1),

I'm seeking your approval for renewing our current Fivecast Onyx open-source intelligence software licensing arrangements for a further 12 months.

s 22(1)

Fivecast is a powerful open-source intelligence solution which uses artificial intelligence processes and deep learning to analyse networks, images, video and threats across multiple sources. The benefits of Fivecast include comprehensive training provided, capability that is used by leading international intelligence agencies in discovering online threats and entities of interest, tradecraft to create online personas all undertaken by the vendor (meaning no staff using their own Facebook or LinkedIn credentials etc.) and ability to directly use intelligence outputs into our existing systems (our SID/Case Management software).

s 22(1)

As this tool has wider applications, we also have provided the Corporate Fraud team one of these licenses to undertake their own integrity work as well. s 22(1)

s 22(1)

s 22(1)

s 22(1)

s 22(1)

s 22(1)
Director

Compliance Intelligence | Skills Programs Compliance and Assurance Branch
Digital Projects, Loans and Compliance Division
Australian Government Department of Employment and Workplace Relations (DEWR)
Phone S 22(1) | Mobile S 22(1)
dewr.gov.au

The Department of Employment and Workplace Relations acknowledges the traditional owners and custodians of country throughout Australia and their continuing waters and community. We pay our respects to them and their cultures, and Elders past, present and emerging.

s 22(1)

s 22(1)

ICT Sourcing Request – ICTSR-23-2536 – s 22(1) -
Department of Employment and Workplace Relations

s 22(1)

Procurement details

Procurement title

Fivecast Onyx Subscription

s 22(1)

s 22(1)

Business case

s 22(1)

Business benefits

This subscription will enhance the business functions of the Compliance Intelligence section.

DTA Policies

s 22(1)

Detailed response

The FiveEyes Onyx package provides the services that the Compliance Intelligence section of the Skills programs Compliance Branch decided will most meet their needs. Included in the procurement is training on the use of the facility in order to make the best use of the investment.

s 22(1)

This cloud-based service is innovative in being a solution to outsource open-source intelligence collection and analysis. As the department is without the ability to collect this data ourselves, the leveraging of the service to provide this level of access is a cost-effective method of obtaining otherwise inaccessible information.

S 22(1)

s 22(1)

s 22(1)

Consider First Assessment Tool

Exported: 21-09-2023

Submission date: 21-09-2023 16:16:09

s 22(1)

Position
Fivecast Onyx Subscription

s 22(1)

s 22(1)

s 22(1)

s 22(1)

Business benefits

This subscription will enhance the business functions of the Compliance Intelligence section.

PRINCIPLE 1

s 22(1)

Write a response to support your answer

The FiveEyes Onyx package provides the services that the Compliance Intelligence section of the Skills programs Compliance Branch decided will most meet their needs.
s 22(1)

PRINCIPLE 2

s 22(1)

s 22(1)

Write a response to support your answer

This cloud-based service is innovative in being a solution to outsource open-source intelligence collection and analysis. As the department is without the ability to collect this data ourselves, the leveraging of the service to provide this level of access is a cost-effective method of obtaining otherwise inaccessible information.

s 22(1)

s 22(1)

s 22(1)

s 22(1)

s 22(1)

s 22(1)



Approval of commitment or expenditure of relevant money

When to use this form? *This form can be used for essentially any proposal to commit or expend relevant money. This form's primary purpose is to assist officials document the necessary accountabilities in the approval of the commitment (spending) of money and the entering, varying or administering of an agreement. Officials must exercise the power to commit or expend relevant money consistently with their duties under section 25 to 29 of the PGPA Act (General Duties of Officials)¹, the Accountable Authority Instructions (AAIs) and with the terms of the delegation or authorisation.*

Requesting officer details

Name:	s 22(1)	Branch:	IT Workplace, Environment & Customer Support	Phone Ext.	s 22(1)
-------	---------	---------	--	------------	---------

Details of the proposed commitment or expenditure of relevant money

Brief description of commitment or expenditure of relevant money	ICTSR 232536 - Fivecast Onyx Subscription for 12 Months. The Fivecast Onyx package provides the services that the Compliance Intelligence section of the Skills programs Compliance Branch decided will most meet their needs. s 22(1) This cloud-based service is innovative in being a solution to outsource open-source intelligence collection and analysis. As the department is without the ability to collect this data ourselves, the leveraging of the service to provide this level of access is a cost-effective method of obtaining otherwise inaccessible information. Fivecast are the OEM and the only provider of this subscription, and as such were approached for quote via the DTA Software Marketplace Panel (RFQ: SM-06940). s 22(1)
--	--

s 22(1)

s 22(1)

² Approval for commitment and expenditure proposal must be obtained prior to entering into contracts or funding agreements. If approval is not obtained prior to entering into the arrangement this should be reported as a breach of PGPA Act section 23 in the department's Financial Management Compliance System, TORQUE.

Delegate Approval

I am satisfied that this proposal promotes the proper use and management of public resources, achievement of the purpose of the department and promotes financial sustainability of the department. I approve the commitment to spend relevant money in my capacity as a delegate under section 23 of the PGPA Act. The approval is subject to the limits and conditions specified in Schedule 1 of department's current financial delegations.

For the purpose of entering into, varying or administering the arrangement, I approve the spending proposal in my capacity as a delegate of: <i>Financial Framework (Supplementary Powers) Act 1997, S32B</i> ☐ <i>Public Governance, Performance and Accountability Act</i> ☒ Check appropriate box ☒ above, noting FFSP Act will be relevant for grant programmes listed in Schedules 1AA and 1AB of the FFSP Regulations.	Section 60 Delegate approval - where required For the purpose of the grant of an indemnity, guarantee or warranty: <i>Section 60, Public Governance, Performance and Accountability Act</i> ☐ Check box ☒ above only if applicable, noting that the approval is subject to the limits and conditions specified in the department's current financial delegations.
---	--

Name	s 22(1)	
Position	Assistant Secretary, IT Workplace Environment and Customer Support Branch.	
Signature	s 22(1)	Date 29-Nov-2023
Conditions for entering into arrangements: Delegate may approve a proposal to spend money subject to conditions which must be complied with by those who subsequently enter into an arrangement e.g. by signing a contract or agreement.		

Software Marketplace contract

Contract

Category: Clause 2 of the Head Agreement
Contract offerings: Clause 9 of the Head Agreement & Schedule 3

Contract ID	SM-06940-FTT
SON	SON3490955
RFQ ID	SM-06940
Category	Software and System Maintenance and Support
Contract title	SM-06940-FTT - Fivecast Onyx Subscription - ICTSR 232536
Buyer internal reference ID	SM-06940-FTT - Fivecast Onyx Subscription - ICTSR 232536
Seller reference ID	SM-06940-FTT - Fivecast Onyx Subscription - ICTSR 232536
Contract offerings	Fivecast ONYX Subscription - 12 months - As per Attachment A

Seller details

Clause 26 and 27.9 of the Head Agreement

Company	Fivecast Pty Ltd
---------	------------------

S 22(1)

Buyer details

Clause 26 and 27.10 of the Head Agreement

Agency / Entity

Department of Employment and Workplace Relations

S 22(1)

S 22(1)

S 22(1)

Subject to third-party review rights

s 22(1)

s 22(1)

s 22(1)

s 22(1)

s 22(1)

s 22(1)

s 22(1)

s 22(1)



Fivecast ONYX

Standard Operating Procedure (SOP)

Introduction

Fivecast ONYX (<https://www.fivecast.com/>) is a Software as a Service (SaaS) that delivers unmatched access to open-source data for intelligence analysis. This document is to provide the overarching procedures and governance structure for the use of Fivecast ONYX (Fivecast) in the Department of Employment and Workplace Relations (DEWR).

Overview

Fivecast ONYX is available via annual licensing subscriptions, with DEWR obtaining 5 licenses to support the objectives of uplifting intelligence capability and as part of the Enhancing Operational Compliance across Skills Programs (EOISP) DCB IT Project 2023-24, led by the Skills Programs Compliance – Compliance Intelligence Team.

Ongoing licensing arrangements will be contingent on the assessment of the product and value derived from intelligence insights from the product.

Roles

Administrator: An administrator (admin) role will perform checks and user audits regularly with the software to ensure compliance with policies and procedures. The administrator will be responsible for communicating any security and policy requirements for new users before providing access and maintaining a Fivecast user register.

User: User roles will have access to Fivecast undertake analysis and use to generate data. These roles will be limited to select personnel from Compliance Intelligence and Corporate Fraud team.

User Register

A Fivecast register will be hosted and maintained for recording all users by the admin. Users will request access via an email to DEWR – Compliance Intelligence mailbox (s 22(1) @dewr.gov.au) and need to provide a business case for demonstrating access is required for their role (Compliance, Intelligence, Counter-Fraud) and aligned with usage approved usage requirements under the Fivecast Privacy Threshold Assessment (PTA).

Users will also be required to advise the admin when they no longer need access to Fivecast. Where access is ceased, or a user account is deactivated the register will be updated to reflect this. Regular usage audits will be conducted by the admin to identify any existing user accounts that are no longer requiring access or are dormant for more than 3 months and may reallocate licenses accordingly. If a user requires access after deactivation has occurred, they will be required to submit a new request via email.

Access

Once access has been approved by the admin, users will be provided the Fivecast link to the website and access their account to create Fivecast investigations. Users will also be provided a link to Fivecast Academy where users can undertake self-directed training on product tradecraft.

Security

Fivecast accounts will be required to use passwords that meet departmental length and complexity requirements as per DEWR's User Access Control Policy. Users on approval will be advised of the DEWR IT Security Policy and minimum password requirements through onboarding documentation as well as being recorded in user register.

Users will also be required to immediately notify the admin in any cases where there is any potential breach of an account or unauthorised disclosure of any information identified that is derived from Fivecast holdings for appropriate escalation. In any cases where a misuse of the software is identified or conflicts with the APS Code of Conduct this will be escalated for appropriate treatment.

Data handling

Data generated from Fivecast is considered open-source information and used for intelligence purposes only. Departmental users when using Fivecast will only identify Information considered relevant as defined in the Fivecast PTA. This information will potentially inform new lines of inquiry and support on-going reviews and investigations on a case-by-case basis. Information viewed in Fivecast will not be used directly as evidence, and where relevant information is identified for a review or investigation the material will generally be assessed and second-sourced outside of the Fivecast software. Users are to contact the admin to seek further clarification if required.

Fivecast information where relevant will be downloaded as a discrete data set directly from the Fivecast User interface and analytical outputs stored in an appropriate DEWR iBase instance, such as the Skills Intelligence Database (SID) or equivalent (CIMS). This ensures the data is handled in compliance with privacy and security framework. Users will also be responsible for determining the appropriate security classification of the Fivecast holdings or any of the analytical products derived.

The use of SID is guided by the SID Privacy impact Assessment (PIA) and all users must ensure Fivecast information held within SID is in line with the PIA and treatments in place with the Skills iBase Database RiskNet-2: Plan 001296.



Australian Government
Department of Employment
and Workplace Relations

Fivecast ONYX - User Policy & Procedures

Fivecast Open Source Intelligence Software -
Policy, Procedures and Guidance on use

ISBN



With the exception of the Commonwealth Coat of Arms, the Department's logo, any material protected by a trade mark and where otherwise noted all material presented in this document is provided under a Creative Commons Attribution 4.0 International (<https://creativecommons.org/licenses/by/4.0/>) licence.

The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the CC BY 4.0 International (<https://creativecommons.org/licenses/by/4.0/legalcode>)

The document must be attributed as the *Fivecast ONYX - User Policy & Procedures*.

Contents

Introduction.....	4
Background.....	4
Fivecast ONYX software.....	4
Fivecast Limitations.....	5
Fivecast Administration.....	5
User Guidance.....	5
Role Based Access Control.....	5
Access Requests.....	6
Users Register.....	6
Role Descriptions.....	6
Administrator.....	6
User.....	6
User Password Requirements.....	6
Appropriate Use and Auditing.....	7
Identified Risks.....	7
Data Handling.....	8
Data Retention.....	8
Fivecast Use Cases.....	9
Document History.....	10

Introduction

This document provides the overarching procedures and governance structure for all staff using Fivecast ONYX in the Department of Employment and Workplace Relations (DEWR).

The term 'all staff' refers to:

- Ongoing employees
- Non-ongoing employees
- Casual employees
- Contractors

Background

Open-Source Intelligence (OSINT) is the process of collecting, analysing, and extracting meaningful insights from publicly available data sources including social media, news feeds, blog sites and discussion forums. The growth of open-source data is exponential and will be for the foreseeable future.

Extracting useful intelligence from open-source data is increasingly challenging for analysts because of the constantly increasing volume, velocity, and variety of data available. As a result, it is now essential for intelligence teams to leverage technical solutions that automate data collection and analysis, in addition to their own analytical expertise and tradecraft, to progress compliance activities and investigations.

Fivecast ONYX is a powerful OSINT solution which uses artificial intelligence processes and deep learning to analyse networks, images, video, and threats across multiple data sources. The product is available via annual licensing subscriptions, with DEWR re-obtaining 5 licenses under the Skills Programs Compliance - Enhancing Operational Intelligence across Skills Programs (EOISP) DCB IT Project 2023-24. The EOISP is led by the Compliance Intelligence Team in collaboration with DSD and TSD to support the objectives of uplifting intelligence capability.

Ongoing licensing arrangements of Fivecast in DEWR will be contingent on the final assessment of the product at the conclusion of the project and value derived from the intelligence insights provided. The current license arrangements will expire in December 2024.

Fivecast ONYX software

Fivecast ONYX (**Fivecast**) (<https://www.fivecast.com/>) is a Software as a Service (SaaS) solution that delivers unmatched access to open-source data for intelligence analysis.

The department has licenses assigned to the following Groups:

- Skills and Training Group (Compliance Intelligence, Skills Compliance Delivery)
- DEWR Corporate and Enabling Services (Fraud)

Additional user groups may also be considered upon request with an appropriate use case.

Fivecast Limitations

Information collected through Fivecast cannot be relied upon as evidence as the software is a discovery tool only. To be relied upon as evidence, the information must be collected and verified by the primary source and handled in a manner that is consistent with DEWR evidence management policies and in alignment with the Fivecast Software Terms of Service.

The Software is a discovery tool, and the information should not be used for evidentiary purposes. All information provided by the Software should be verified by the primary source of the information.

Fivecast Administration

As Fivecast is a specialised intelligence tradecraft capability and engaged as part of the EOISP, the role of Administrator (admin) is being undertaken in the program area intelligence team. As of 8 January 2024, the Director, Compliance Intelligence is the current Administrator and Business Owner of Fivecast.

The vendor will provide training and access to Fivecast users on commencement and provide access to the training academy for ongoing learning and development.

User Guidance

Fivecast users should only collect information that is relevant to a user's allocated or agreed project, investigation or intelligence project. Fivecast must not be utilised by any users to look up people not associated with a project or intelligence activity or investigation. Misuse of the software by staff, including searching for individuals without a business requirement to do so, may result in their access being revoked and potential disciplinary action.

Each team holding a licence for Fivecast is responsible for:

- implementing an approach for approving searches to be undertaken
- reviewing their collated data stored in Fivecast which should be undertaken periodically
- deleting data in Fivecast when a project is completed, a compliance activity concluded, or an investigation has been closed (should there be no evidence keeping requirements in effect as dictated by other policies and legislative requirements).

Reviews of data holdings for a team can be made to the Administrator at any time.

Role Based Access Control

Access to Fivecast ONYX considers a Role Based Access Control (RBAC) model that aligns with the roles and functions that the user performs in – such as Compliance, Integrity and Fraud related functions and must align with the approved usage requirements under the [Fivecast Privacy Threshold Assessment](#) (PTA). The Fivecast privacy assessment is reviewed quarterly to ensure currency and accuracy. Only staff required to have direct access to the system, are given access by following the “need-to-know” principle. Additionally, the “least-privileged” principle applies in provisioning access.

Access Requests

The staff onboarding and offboarding procedure is that Fivecast Users must advise the admin when they are seeking access to or no longer require access to Fivecast. The admin will also maintain and update a Fivecast user register.

Users will request Fivecast access via an email to the DEWR – Compliance Intelligence mailbox (s 47G(1)(a) [@dewr.gov.au](mailto:compliance@dewr.gov.au)) and need to provide a business case for demonstrating access is required for their role (Compliance, Intelligence, Investigations, Counter-Fraud).

Where access is ceased, or a user account is deactivated the register will be updated to reflect this. If a user requires access after deactivation has occurred, they are required to submit a new request via email.

On issue of a Fivecast account a copy of this document and access instructions will be provided to the user.

Users Register

The Fivecast Administrator will maintain a current register of Fivecast users to ensure that the licenses (currently 5) are allocated and assigned to staff. The details of the register will include:

ID	Team	Name	Email	User Account ID	Start Date	End Date
----	------	------	-------	-----------------	------------	----------

A copy of the User Register is available on request from the admin where appropriate.

Role Descriptions

There are two primary roles assigned for Fivecast – *Administrator* and *User*:

Administrator

An administrator (admin) role will perform checks and user audits regularly with the software to ensure compliance with policies and procedures. The administrator will be responsible for communicating any security and policy requirements for new users before providing access and maintaining a Fivecast user register.

User

User roles will have general access to Fivecast to undertake analysis and generate data. These roles will be limited to selected personnel with a sufficient business case from Compliance Intelligence and Corporate Fraud team.

s 47E(d)

s 47E(d)

Appropriate Use and Auditing

Staff must comply with DEWR's Acceptable Use of IT Policy and compliance rules. Users will also be required to immediately notify the admin in any cases where there is any potential breach of an account or unauthorised disclosure of any information identified that is derived from Fivecast holdings for appropriate escalation. In any cases where a misuse of the software is identified or conflicts with the APS Code of Conduct this will be escalated for appropriate treatment.

Regular usage audits will be conducted on a 3-months cycle (Jan-Mar, Apr-Jun, Jul-Sep, Oct-Dec) by the admin to identify access and appropriate usage.

Any existing user accounts that are no longer requiring access or are dormant for more than 3 months may be deactivated to reallocate licenses accordingly.

Identified Risks

Staff members using Fivecast to collect information on parties with no relevance to business requirements (including but not limited to - acquaintances, ex-spouses, or family members) is considered a risk. Any staff member being identified as using the Fivecast software inappropriately should have appropriate disciplinary action taken against them, including:

- issuance of a formal Security Breach
- temporary suspension of access rights to Fivecast resources
- referral to the Performance and Conduct Team for possible disciplinary action in accordance with APS Code of Conduct
- referral to AGSVA, by which the ASA may consider a Review for Cause to assess suitability to continue to hold a Security Clearance; and/or
- disciplinary action against contractors in accordance with the terms of their contracts.

Please consult the [Plan of Action and Milestones - Fivecast ONYX \(PoAM\)](#) for further information of identified IT risks and treatments.

Data Handling

Data generated from Fivecast is considered open-source information and used for intelligence purposes only. Departmental users when using Fivecast will only identify information considered relevant (as defined in the Fivecast PTA). This information will potentially inform new lines of inquiry and support on-going reviews and investigations on a case-by-case basis. Information viewed in Fivecast will not be used directly as evidence, and where relevant information is identified for a review or investigation the material will generally be assessed and second-sourced outside of the Fivecast software. Users are to contact the admin to seek further clarification if required.

Exporting and saving of files produced within Fivecast ONYX (including screenshots captured) are to be saved and downloaded as a discrete data set directly from the Fivecast User interface and analytical outputs stored in an appropriate DEWR iBase instance, such as the Skills Intelligence Database (SID) or equivalent (CIMS). This ensures the data is handled in compliance with privacy and security framework with existing audit controls and procedures are in place (including additional resource group management and user access controls). Users will also be responsible for determining the appropriate security classification of the Fivecast holdings or any of the analytical products derived.

The use of SID is guided by the SID Privacy impact Assessment (PIA) and all users must ensure Fivecast information held within SID is in line with the PIA and treatments in place with the Skills iBase Database RiskNet-2: Plan 001296.

Training will be provided by the vendor on commencement and Fivecast Academy access (self-paced training) is also provided. A Task Card document will also be created to document the process for Fivecast users using SID that will align with equivalent DEWR i2 iBase systems (such as CIMS).

Data Retention

All data collected by the vendor for DEWR and stored in the cloud holdings will be deleted by Fivecast once the department's licences expire or are terminated. Other than this, all collected information remains visible to the User and stored on the server allocated to the department.

While Fivecast cannot access information other than what is publicly available, information that is collected by the department must also be handled in accordance with the Privacy Act 1988.

Subject to third-party review rights

Document History

Version	Date	Author	Summary of Changes
0.1	29 March 2021	s 22(1)	First Draft
1.0	20 April 2021	s 22(1)	Finalised version with accepted changes in version 0.1 incorporated
1.1	11 June 2021	s 22(1)	Addition of current users
1.2	21 March 2022	s 22(1)	Updates to include a whole of department approach and revisions to Administrator and Users
1.3	30 April 2022	s 22(1)	Updates to users, licenses, platforms and edits from child care.
2.0	29 August 2023	s 22(1)	Updated content to reflect new requirements, processes and PTA.
2.1	8 January 2024	s 22(1)	Updated from original DESE “Fivecast ONYX User Policy – 2022”. Updates include Cyber Assurance recommendations and requirements (Plan of Action and Milestones - Fivecast ONYX). Removed the user register details due to sensitivity.
2.2	9 January 2024	s 22(1)	Updated minor edits and formatting.

Fivecast Onboarding - Email Template

Tuesday, 9 January 2024 1:14 PM



DEWR
Fivecast O...

Admin to send via S 22(1)

@dewr.gov.au mailbox

Good Morning/Afternoon USER,

Welcome to using Fivecast ONYX (Fivecast) in the Department of Employment and Workplace Relations (DEWR). A Fivecast User Account has been provided to you as an appropriate business requirement for using the software has been determined (Compliance, Intelligence, Investigations and/or Integrity purpose).

Fivecast is a specialised open-source intelligence tradecraft capability that is being provided by the Compliance Intelligence team as part of the 2023-24 Capital IT Project 'Enhancing Operational Intelligence across Skills Programs' (EOISP). The use of Fivecast allows a user to search across these multiple platforms simultaneously without requiring the creation of log in details (managed pools via Fivecast) and without overtly exposing the Department's interest in entities to third party companies. It provides a platform for this information to be consolidated more efficiently and a safe way to access it with no direct engagement with social media platforms themselves. The information is only to be accessed by authorised departmental staff and where relevant material is derived it is to only be recorded and secured in an appropriate DEWR case management environment (such as SID or CIMS).

Attached is the **Fivecast ONYX - User Policy & Procedures** document that you are required to familiarise yourself with to ensure ongoing compliance with the Policy, Procedures and Guidance on using this product. The Administrator will also maintain the Fivecast user register with routine auditing (see the Policy & Procedures document for additional details). A copy of the Fivecast Privacy Threshold Assessment (PTA) can also be provided on request.

Your Fivecast Log-In Credentials are as follows:

Fivecast ONYX

User Name:	XXXXXX
One-time Password:	XXXXXX

Fivecast Academy (training)

User Name:	XXXXXX
One-time Password:	XXXXXX

A Fivecast first-time user guide is provided in the below email. We also anticipate the vendor delivering a training workshop once users have been onboarded as well (expected by end-January 2024) and creation of a Task Card for Fivecast information processes in the Skills Intelligence Database (SID) or i2 iBase equivalent (CIMS).

All Users must advise the Fivecast Administrator via the S 22(1) @dewr.gov.au mailbox when access to the Fivecast software is no longer required. Any questions on storage, use, disseminations or legal considerations of Fivecast information should also be directed to the mailbox for further consultation. Any breaches or misuse identified must also be reported immediately as per DEWR's IT User Policy.

Please contact the mailbox for any further questions, issues or concerns.

Thank You,

(Fivecast Admin)

The Department of Employment and Workplace Relations acknowledges the traditional owners and custodians of country throughout Australia and their continuing connection to land, waters and community. We pay our respects to them and their cultures, and Elders past, present and emerging.

Subject to third-party review rights

Subject to third-party review rights

Subject to third-party review rights

Subject to third-party review rights

Subject to third-party review rights