

Commitment Approval Minute

TO: s47E(c), s47F, Director, Procurement and Software Commercials Section (PSC)
Enterprise Portfolio Management and Commercial Branch (EMPC)
Digital Services within Corporate Operations Group

COMMITMENT APPROVAL TO PURCHASE 3 X FIVECAST ONYX PRO LICENCES THROUGH FIVECAST PTY LTD FOR A 12-MONTH PERIOD.

PURPOSE

This Minute recommends that you:

- R1. APPROVE** the indemnity clause in the contract which is in favour of Fivecast Pty Ltd in accordance with section 60 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), as outlined in the Section 60 Assessment section of this minute. The terms and conditions of the EULA, including indemnity, are assessed as MEDIUM risk as per **Attachment A**;
- R2. APPROVE** the expenditure of Departmental funds of **\$107,250.00 (GST inclusive)**, for the purchase of three Fivecast Onyx Pro licences from Fivecast Pty Ltd (**ABN: 48 621 030 199**), under Section 23(3) of the PGPA Act;
- R3. NOTE** the quotation/proposal from Fivecast Pty Ltd at **Attachment B**;
- R4. NOTE** the funds availability confirmation at **Attachment C**;
- R5. NOTE** Fivecast Onyx Pro has been approved for use within the Department (Enterprise Architecture and Cyber Security) via Cherwell ticket 4035187;
- R6. NOTE** the mechanism of purchase will be issuing a purchase order that operates under the terms and conditions of the End User Licensing Agreement (EULA) at **Attachment A**; and
- R7. SIGN** the attached manual purchase order at **Attachment D**.

1. SECTION 60 PGPA ACT APPROVAL

Contracts which contain a contingent liability cannot be entered into without being approved in accordance with s60 of the PGPA Act.

Table 3 of Schedule 1 of the Departments Delegations states that the Section 23(3) delegate for any engagement also has the Section 60 delegation for that same engagement. Resultantly, you have the Delegation to approve the indemnity clause in this agreement. Accountable Authority Instructions 2.2 and Finance Business Rule R2.2 provide the Department's rules and guidance for assessing risk and providing section 60 Approval.

s47E(d)

s47E(d)

It is recommended that Section 60 Approval is provided in accordance with the Finance Business Rule R2.2 and as per Department Financial Delegations to address the PGPA Section 60 requirement.

Please note that if you decide against providing section 60 approval then you are unable to provide section 23(3) approval to procure licenses from Fivecast Pty Ltd.

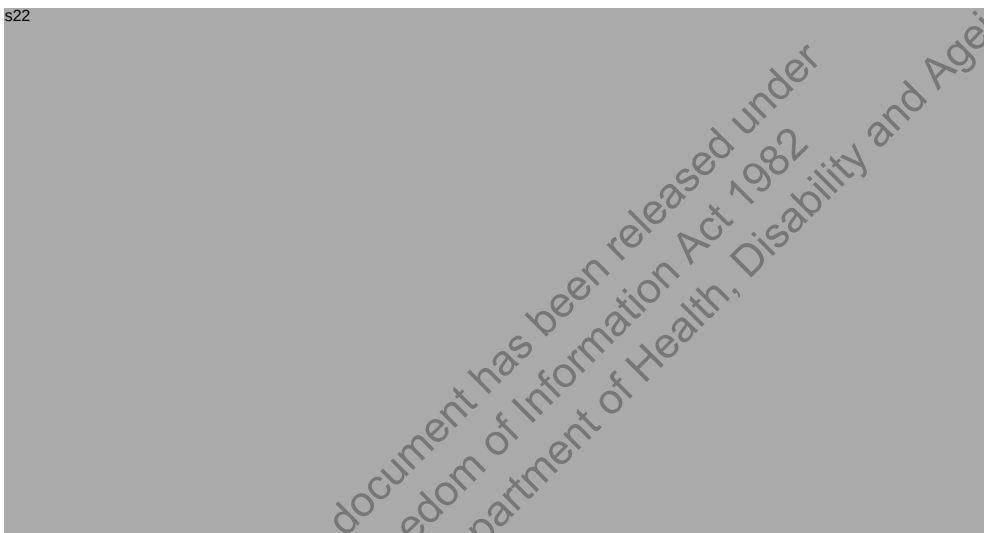
2. BACKGROUND/CONTEXT

To address the growing complexity and volume of intelligence referrals, the Therapeutic Goods Administration (TGA) Intelligence Team requires advanced Open Source Intelligence (OSINT) tools to enhance its operational capabilities. Current manual methods of data collection are time-consuming, limited in scope, and increasingly inadequate for identifying non-compliant activities across digital platforms.

Fivecast Onyx offers transformative capabilities including deep web access, cross-platform social media analysis, and automated data aggregation, which significantly reduce turnaround times and improve the accuracy and depth of intelligence reporting. Investing in this tool will enable the team to deliver timely, comprehensive intelligence products, support strategic regulatory functions, and achieve greater efficiency than would be possible through additional staffing alone.

Fivecast Onyx is used by a number of federal government agencies including:

s22



A proposal has been prepared by the vendor (**Attachment B**). This requirement has been confirmed by the relevant business owner s47E(c), s47F, Regulatory Practice and Support Division.

3. TIMEFRAME

Support and maintenance for Fivecast Onyx Pro will be provided from 1 July 2025 – 30 June 2026.

4. VALUE FOR MONEY

The proposed OSINT tool, FIVECAST Onyx, was identified by the Department's Intelligence Forum as a preferred solution due to its proven use across other government agencies and its advanced capabilities, including dark web access, AI-driven analytics, and secure persona-based investigations. These features significantly surpass the limitations of manual intelligence methods. The decision to proceed with Fivecast Onyx was informed by qualitative feedback from analysts, its alignment with key intelligence priorities—such as timeliness, reach, and reliability—and a thorough review of licensing and implementation costs. It offers a scalable solution that enhances the TGA's intelligence capability while delivering a strong return on investment. Accordingly, the purchase of these licenses represents value for money to the Department.

5. CONTRACTUAL ARRANGEMENT

The licenses will be purchased via the issuing of a purchase order and will be provided under the conditions of the EULA. The nominated Contract Manager for this arrangement will be the Director,

Procurement and Software Commercials Team, EPMC. Business Ownership and approval given through s47E(c), s47F, Director, Governance and Integrity Section, Regulatory Practice and Support Division.

6. COMPLIANCE WITH COMMONWEALTH PROCUREMENT RULES

This procurement is above the relevant threshold (\$80,000.00 GST inclusive) and therefore the additional rules for procurements at or above the relevant procurement threshold in Division 2 of the Commonwealth Procurement Rules will apply. The Value for Money considerations found in Division 1 have been applied.

The Commonwealth Procurement Rules state that Commonwealth entities must only conduct a procurement at or above the relevant procurement threshold through limited tender when a specific condition for limited tender is met. In this instance, the relevant conditions for limited tender are as follows:

- 10.3.d - when the goods and services can be supplied only by a particular business and there is no reasonable alternative or substitute for one of the following reasons:*
- ii. to protect patents, copyrights, or other exclusive rights, or proprietary information; AND*
 - iii. due to an absence of competition for technical reason*

Fivecast software provides an open-source intelligence platform for obfuscated monitoring and collection of publicly available information. This is proprietary software and no suitable alternative is available from any vendor.

7. INDIGENOUS PROCUREMENT POLICY

The expected value of the procurement is between \$80,000 and \$200,000, however, this procurement uses a 10.3 exemption, so the mandatory set-aside does not apply.

8. EXPENDITURE APPROVAL AND FUNDS AVAILABILITY

The cost to the Department for this purchase is **\$107,250.00** (GST inclusive). This is within your delegation limit under the Accountable Authority Financial Delegations Schedule 1, Table 1, Item 54, to approve proposals to commit relevant money up to \$1,000,000.00.

Cost Centre	Cost Centre Name	Funding Type	GL Code	Internal Order	Expenditure (GST Inclusive)
TG00000114	MRD PB TECHNICAL	Departmental	5200001644	N/A	\$107,250.00

The Finance Business Partner has confirmed that funds are available at **Attachment C**.

Forward Commitment

Beyond Forward Estimates Approval is the approval of funds beyond the forward estimates period (current financial year plus four financial years out). It is a requirement under instruction from the Secretary (S16 PGPA Act- Schedule Instruction 1), the Department's Financial Delegations and Finance Business Rules.

As the duration of the expenditure proposal does not extend beyond the forward estimates period, a Beyond Forward Estimates approval has not been completed. In addition, this commitment approval does not contain any contingent liabilities.

9. GENERAL

The risk profile for this procurement process is MEDIUM, based on the EULA Risk Review at **Attachment A**. There are no additional procurement risks associated with this process. There are no known conflict of interest issues that have been raised throughout the process. Any significant risks and mitigations identified will be advised to the delegate.

Internal Reporting Requirements

Under the Department's Procurement Processing and Management policy, contracts must be registered within 2 business days of execution.

External Reporting Requirements

The contract will be reported on the Department's website in accordance with the Senate Order requirements of July 2001 (Murray Motion). As the contract is valued over \$10,000 it will be reported on AusTender within 42 days of entering into the contract, in line with the Commonwealth Procurement Rules (Division 1, Item 7, Reporting arrangements).

Documentation

The documentation is held on TRIM File E25-342774. All relevant documentation has been filed in accordance with [Corporate Business Rule 2: Information Management and Record Keeping](#).

Prepared by:

s47E(c), s47F

Procurement and Software Commercial
Enterprise Portfolio Management and Commercial Branch
Date: 30 June 2025

s47F

s47E(c), s47F

Director, Governance and Integrity Section
Regulatory Practice and Support Division
Date: 30 June 2025

10. DELEGATE APPROVALS

It is recommended that you, as delegate:

- R1. **APPROVE** the indemnity clause in the contract which is in favour of Fivecast Pty Ltd in accordance with section 60 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), as outlined in the Section 60 Assessment section of this minute. The terms and conditions of the EULA, including indemnity, are assessed as MEDIUM as per Attachment A;
- R2. **APPROVE** the expenditure of Departmental funds of \$107,250.00 (GST inclusive), for the purchase of three Fivecast Onyx Pro licences from Fivecast Pty Ltd (ABN: 48 621 030 199), under Section 23(3) of the PGPA Act;
- R3. **NOTE** the quotation/proposal from Fivecast Pty Ltd at Attachment B;
- R4. **NOTE** the funds availability confirmation at Attachment C;
- R5. **NOTE** Fivecast Onyx Pro has been approved for use within the Department (Enterprise Architecture and Cyber Security) via Cherwell ticket 4035187;
- R6. **NOTE** the mechanism of purchase will be issuing a purchase order that operates under the terms and conditions of the End User Licensing Agreement (EULA) at Attachment A; and
- R7. **SIGN** the attached manual purchase order at Attachment D.

Delegate Approval

s47F

s47E(c), s47F

Director, Procurement and Software Commercials Section (PSC)
Enterprise Portfolio Management and Commercial Branch (EMPC)
Digital Services within Corporate Operations Group

30.06.2025

Date:

Attachments:

ID	Description	Trim Ref
A	EULA Risk Review	D25-2811245
B	Quotation/Proposal	D25-2789391
C	Funds availability confirmation	D25-2791026
D	Manual Purchase Order	D25-2817505

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

HPRG Intelligence – Nexus Xplore/Onyx FIVECAST Procurement

Rank: XX (Value)

Branch	HPRG – Represented by Regulatory Compliance Branch	Program	1.8 Health Protection, Emergency Response and Regulation	Funding Status	Funding available	Lifecycle Stage	Procurement
Decision Requested	Approval to progress to procurement for Nexus Xplore and Onyx FIVECAST for HPRG Intelligence						
Committee Decision							

Altus ID	
SRO	Tracey Lutton
PM	s47E(c), s47F

What?	Description	Key Activities/Outputs/Scope Items			Key Documents	
	- HPRG Intelligence conducts complex open-source intelligence collection to further attribute persons of interest to their non-compliance activities. - The Departmental network is not suitable for broader collection activities because many websites are flagged and blocked. - HPRG Intelligence seeks to acquire dedicated open-source search and collection software to increase capabilities and efficiency on a secure, non-attributable platform.	- HPRG Intelligence has undertaken testing for both platforms to test accuracy, efficacy and information return. Although the tools share some similarities, they have enough differences to warrant obtaining licenses for both. After the initial license period, the Intelligence team could further assess the continuing need for both tools. - Discussions with IT/Cybersecurity and network architecture teams around implementation and access to the solution via the Departmental network. - Allocation of licenses to analysts and implementation department specific training for Intelligence analysts. - Regular audit to ensure compliance with policies.				
Why?	Benefits (non-financial)	Benefits (financial)			Implementation Risks (Low/Medium/High)	
	- An off the shelf platform such as Fivecast and/or NexusXplore provide a single point of OSINT collections and assessment. This provides significant efficiency gains throughout the collection process. - By embracing OSINT tools, we can anticipate significant efficiency dividends and an opportunity to significantly enhance our influence on future TGA regulatory functions. - The potential benefits of OSINT tools are essential and transformative, promising a more effective and proactive regulatory approach.	- The amount of data that can be obtained using this tool in a matter of hours, rather than days, will allow for faster turnaround on high-priority cases. This not only saves time but also significantly increases the productivity of our analysts, allowing them to focus on more strategic tasks. - The cost of one tool is equivalent to a full-time EL1, but it will provide far more benefit than an additional ASL. - An industry backed and supported platform, with ongoing development, will minimise the likelihood of the system becoming outdated or ineffective for the TGA, minimising the likelihood of future procurement activities.			- Low - Running third-party software on Departmental networks comes with cybersecurity risks (cybersecurity consulted) Note – Information used to search platforms, is identical to information used in current search methods by HPRG Intelligence.	
How?	Dependencies	Architecture Alignment	Resourcing	Costs	Funding	Timeline
	- The procurement of OSINT platform/s are a standalone process with no required project-based work outside of IT Security, Cybersecurity and architecture approval of the systems. - Procedures specific to HPRG Intelligence in relation to dissemination of platform collected information may be required. SOP's will be developed by HPRG Intelligence.	Proposed solution will ensure data security is established in line with the data and architecture governance frameworks.	Discovery: HPRG Intelligence has already undergone testing of the two potential platforms. Implementation: New Sustainment: New	Discovery: \$Nil Implementation: Final costs will be identified during procurement. Sustainment: \$ Total: [If moving to implementation]	Branch budget: funding available in RPSD 2024-15 budget	Start date: End date: Key dates: [Contract renewals, delivery milestones, Go live, etc]

From: LUTTON, Tracey
To: s47E(c), s47F
Cc:
Subject: FW: TRIM: RE: RCB AND WIEB Product - for consideration and approval - OSINT Intelligence Tool [SEC=OFFICIAL]
Date: Friday, 27 June 2025 3:58:03 PM
Attachments: [image001.png](#)
[image002.png](#)
[image003.png](#)

Hi s47E(c),
s47F

As below and discussed – Band 2 support and approval for the spend for both NexusXplore and FIVECAST Onyx.

Thanks

Tracey

Tracey Lutton

Assistant Secretary, Regulatory Compliance Branch

Regulatory Practice and Support Division | Health Products Regulation Group
Australian Government Department of Health, Disability and Ageing

T: 02 s47F | E: tracey.lutton@health.gov.au

Location: 27 Scherger Drive, Fairbairn, ACT

Office s47E(c),
s47F

PO Box 100, Woden ACT 2606, Australia

Executive Support: s47E(c), s47F

E: s47E(c), s47F @health.gov.au

I may send emails out of hours at a time that suits me. I look forward to receiving your response during your normal working hours.

The Department of Health, Disability and Ageing acknowledges the Traditional Custodians of Australia and their continued connection to land, sea and community. We pay our respects to all Elders past and present.

From: BEDFORD, Chris <Chris.Bedford@health.gov.au>

Sent: Wednesday, 9 April 2025 12:35 PM

To: LUTTON, Tracey <Tracey.Lutton@health.gov.au>; MCLACHLAN-BENT, Ashley <Ashley.MCLACHLAN-BENT@health.gov.au>

Cc: s47E(c), s47F @health.gov.au; s47E(c), s47F @health.gov.au

Subject: TRIM: RE: RCB AND WIEB Product - for consideration and approval - OSINT Intelligence Tool [SEC=OFFICIAL]

Thanks Tracey.

I am supportive. We can all discuss, but the funding this financial year shouldn't be a problem, going forward we will have more pressures and if the year 1 use demonstrates significant efficiency etc, then we may need to look at how ongoing use is offset by an ASL etc.

Cheers, Chris

Chris Bedford (He/Him)

First Assistant Secretary

Regulatory Practice & Support Division

Health Products Regulation Group

Australian Government Department of Health & Aged Care

P: 02 5132 0659 | M: s47E(c), s47F | E: Chris.Bedford@health.gov.au

Location: Gulgana Building, Fairbairn, Canberra

GPO Box 9848, Canberra ACT 2601, Australia

Executive Assistant | s47E(c), s47F

P: 02 5132 s47E(c), s47F @health.gov.au

Executive Officer | s47E(c), s47F

P: 02 5132 s47E(c), s47F @health.gov.au

The Department of Health and Aged Care acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

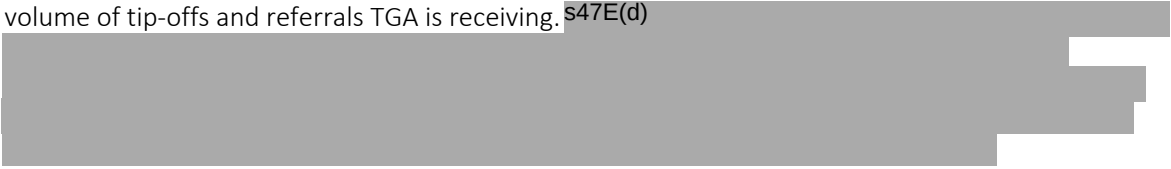
[illegible]

● s22

Tracey

The HPRG Intelligence team offers strategic, operational, and tactical support to both RCB and VIEB.

The intelligence team is currently facing significant challenges due to the increasing complexity and volume of tip-offs and referrals TGA is receiving. s47E(d)



Intelligence objectives

The HRRG Intelligence Team aims to produce value-added intelligence to answer key intelligence questions pertinent to the **TGA Advertising, Import and Supply Compliance Priorities** and RCB and VIEB investigations.

s47E(d)



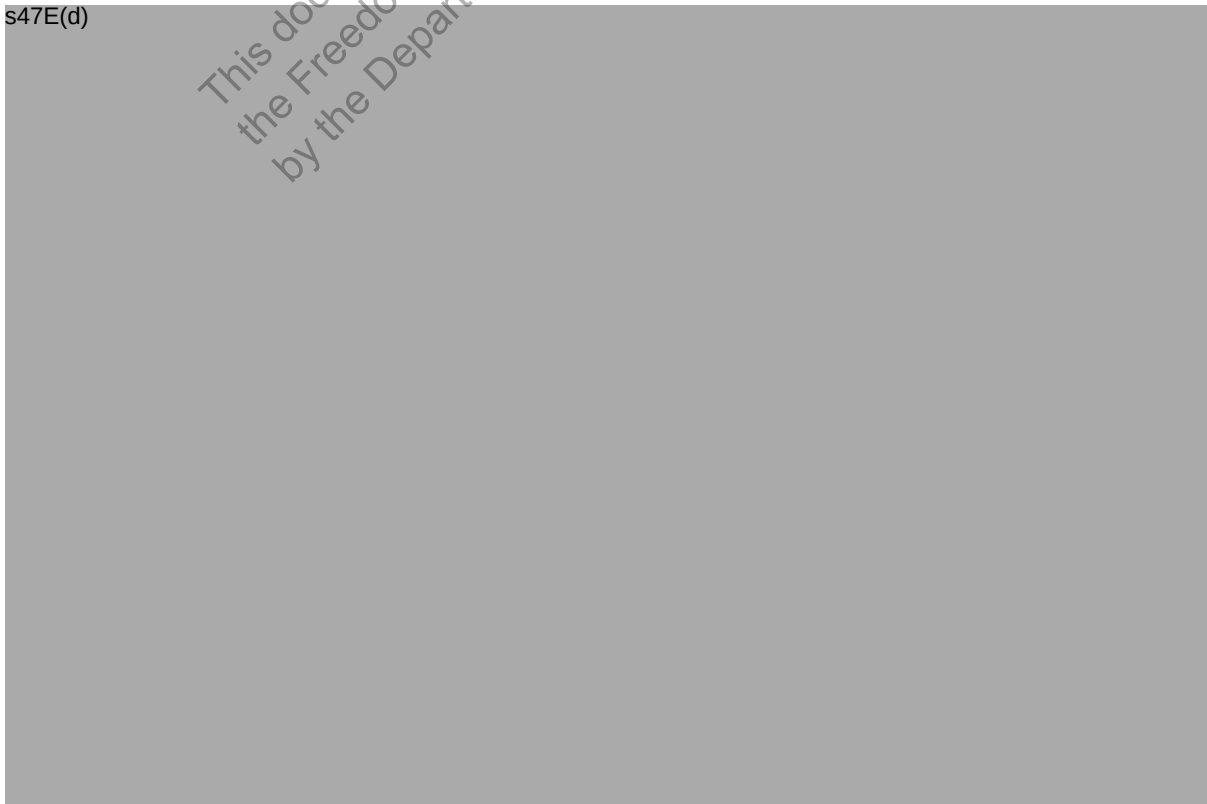
s47E(d)



OSINT Tools

OSINT tools exponentially expand data volumes and provide deeper insights into this ever-increasing set of data. **These tools allow us to do things we cannot do manually.** The benefits of OSINT tools are plentiful:

s47E(d)



This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

Time Savings

- The time savings with the OSINT tools are significant. s47E(d)

- s47E(d)

Options and Analysis

There is a community of practice with other intel areas in the Department, with monthly engagement.

- As a group, they are looking at future resourcing together:
 1. **RCB Intel** - have responsibility for the capability uplift s47E(d)
 2. **Fraud and Integrity** - s47E(d)
 3. **Benefits Integrity** - s47E(d)

Interagency discussion and online research identified two potential vendors offering services highly conducive to TGA regulatory work.

Testing

The intel team has undertaken testing of two OSINT tools from these vendors:

- FIVECAST Onyx and
- NexusXplore

The Intelligence team undertook a work-based assessment of these two OSINT software platforms to ascertain the best fit for purpose and value for money (see attachment – HPRG Intelligence – OSINT Test Review for the full comparative assessment). Both tools aim to give analysts a significant edge by delivering rich, relevant, and accurate information that the intelligence team can use for intelligence assessments.

s47E(d)

Although the trial period for both products offered valuable insights into their usefulness, the complete potential of these tools has yet to be fully realised. We believe that they could have a significant impact in the digital disruption arena, particularly in streamlining processes and enhancing operational efficiency. However, until the team conducts a thorough exploration of all the features and functionalities, we cannot determine the true scope of the benefits the tools may offer. Our

ongoing assessment will be crucial in uncovering their capabilities and understanding how they can best serve our objectives in this rapidly evolving digital landscape.

Proposal

Incorporating an OSINT product into our processes and procedures would allow us to **deliver more timely and comprehensive intelligence**, including relevant information on entities of interest and associations, identification of patterns and trends, and insights into emerging threats and vulnerabilities. The potential benefits of OSINT tools are significant and promising.

By embracing OSINT tools, we can anticipate significant efficiency dividends and an opportunity to significantly enhance our influence on future TGA regulatory functions. The potential benefits of OSINT tools are essential and transformative, promising a more effective and **proactive** regulatory approach.

- The intelligence team currently has a relatively small footprint (6 ASL + grad).
- Each OSINT tool will cost between \$130,000 and \$250,000 pa. **Note:** the final costs will not be available until we engage with the vendor
- The cost of one tool is equivalent to a full-time EL1, but it will provide far more benefit than an additional ASL.
- The original vaping NPP included funding for tools; however, it appears that RCB did not receive this funding. It is our understanding that VIEB has an underspend for 2024-25. The OSINT tools would be a beneficial use of these funds.

Option 1 - Purchase both tools

Although the tools share some similarities, they have enough differences to warrant **obtaining licenses for both**. After the initial license period, the Intelligence team could further assess the continuing need for both tools.

[REDACTED] s47E(d)

Option 2 - Purchase one tool

Although both tools can address important capability gaps, **NexusXplore** aligns best with the team's current needs.

[REDACTED] s47E(d)

Digital Services Prioritisation Board Assessment

If we are to progress to the procurement process, the newly established Digital Services Prioritisation Board (DSPB) must assess and endorse the 'plan on a page' document. The DSPB has been put in place to improve the Governance of departmental digital investment decisions, driving:

- Greater user adoption of sustainable digital solutions.
- Improved collaboration with customers and cross-functional teams.

Recommendation:

That you:

- Agree and provide **in-principle-approval** to proceed with **Option 1** purchase licences for both NexusXplore and FIVECAST Onyx.
- If you agree in principle, the next step is for the DSPB to consider it. A draft 'plan on a page' is will be drafted in accordance with approved option.

FYI – RCB can only afford half of one tool – if you are in agreement to purchase both tools – I'm hoping there's so NPP funding still available we can attribute some money towards?

Thanks

Tracey

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

OFFICIAL: Sensitive

Australian Government
Department of Health and Aged Care
Therapeutic Goods Administration

Health Products Regulation Group

Regulatory Compliance Branch

Comparative Assessment – NexusXplore and Onyx

RCB has identified a clear need for a robust OSINT software platform as part of our broader effort to enhance situational awareness and intelligence gathering. The growing importance of digital environments and the volume of publicly available data means that effective use of OSINT can provide significant advantages.

OSINT Combine NexusXplore and Fivecast Onyx were identified as two OSINT platforms that would likely suit these needs. Intelligence staff members had used one or both of these platforms in previous roles, both platforms were known to be used within other Australian government and law enforcement agencies, and both platforms were recognised by the IT panel.

HPRG Intelligence undertook a work-based assessment of these two OSINT software platforms to ascertain best fit for purpose and value for money. The following is an overview of the findings.

s47E(d)

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

OFFICIAL: Sensitive

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

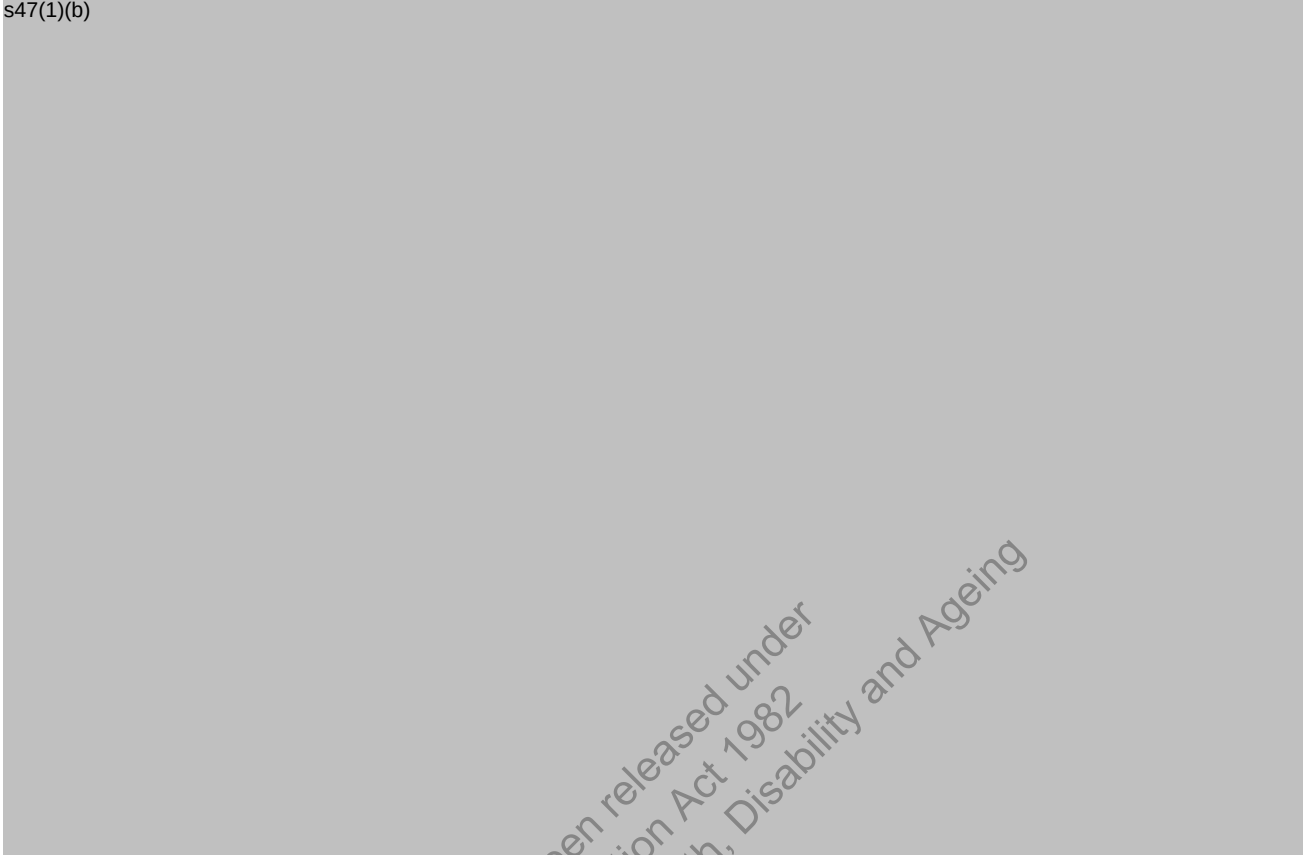
OFFICIAL: Sensitive

Costs

Costings, based on 7 licenses, were provided to HPRG Intelligence in January 2025 as an estimate.

Please note that these numbers are indicative and may vary.

s47(1)(b)



This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

OFFICIAL: Sensitive



Australian Government
Department of Health and Aged Care

Summary of Business Requirements

Request Title: Request Name – (Cherwell:)

Date advice required / reason:

Business Contact: s47E(c), s47F Ph: 02 s47E(c), s47F E: s47E(c), s47F [@health.gov.au](mailto:s47E(c), s47F@health.gov.au)

SN - Several

BR – Regulatory Compliance Branch (RCB) and Vaping Implementation and Enforcement Branch (VIEB)

DIV – Regulatory Practice and Support Division

ITD Front Door Contact: [Insert] Ph: [Insert] E: [Insert]

Background:

High level description of the role/responsibility of the business area in relation to the request. What changes or decisions have taken place to that impact current business process? Note key dates associated with policy decisions and legislated deadlines for implementation.

TGA investigators undertake online investigations to assess non-compliance under the Act and collect evidence. s47E(d)

Issue:

Describe the issue including:

- Function requiring IT support
- Current support for this function
- Key issues / pain points
- Progress completed to date including identified solution options and contingencies

TGA investigators require an IT solution to allow them to access websites s47E(d)

- s47E(d)

Stakeholders:

Complete a table describing the Role and description of interaction with the solution

Title	No.	Role in process	Internal/ external
RCB branch		Investigations / Compliance	Internal
VIEB branch		Investigations / Compliance	Internal

Requirements:

Document high level business requirements which may include the following:

- Access: internal, external, role based.
- Access to secure document storage
- Data capture
- Web site/Online forms
- Document creation / templates
- Workflow / milestone tracking
- Payments / Invoicing
- Approvals
- Reporting
- Integration with other systems (outlook, SAP etc.)

BR	Description	Priority
BR-01	Misattributed website access	1
BR-02	Ability to transfer evidence to Departmental systems	2
BR-03	Ability to access any website	3
BR-04	Online portal accessible through the Departmental network	4
BR-05	Ability to audit user's activities	5
BR-06		
BR-07		
BR-08		

Non-Functional Requirements:

- Security
- Availability
- Accessibility

- Volumetrics
- Support/ maintenance/ restoration timeframes
- Audit
- Performance
- Archive

TEMPORARY

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

From: s47E(c), s47F
To: FRISBY, Jennifer; Digital Services Prioritisation Board; CHESHER, Amanda
Cc: HOBBSIN, Damien; s47E(c), s47F; LUTTON, Tracey; s47E(c), s47F; BEDFORD, Chris; s47E(c), s47F
Subject: RE: Response by 13th May: HPRG Intelligence - Nexus Xplore/Onyx FIVECAST Procurement [SEC=OFFICIAL]
Date: Wednesday, 14 May 2025 3:05:50 PM
Attachments: image001.png
 image002.png
 HPRG Intelligence Nexus Xplore - Onyx Fivecast - Authority to Proceed.docx

Good afternoon All,

Please find attached the signed and approved Authority to Proceed (ATP) for the HPRG Intelligence - Nexus Xplore/Onyx FIVECAST.

Regards,

s47E(c), s47F

Cyber Security Advisor (Contractor)
 Cyber Security Branch | Information Technology Division
 Digital Services within Corporate Operations Group
 Australian Government Department of Health and Aged Care
 T: s47E(c), s47F @health.gov.au
 Location: Yaradhang Level 2 N 8105

From: FRISBY, Jennifer <Jennifer.FRISBY@Health.gov.au>
Sent: Wednesday, 14 May 2025 9:09 AM
To: s47E(c), s47F @Health.gov.au; Digital Services Prioritisation Board s47E(d) @health.gov.au; CHESHER, Amanda <Amanda.CHESHER@Health.gov.au>
Cc: HOBBSIN, Damien <Damien.HOBBSIN@Health.gov.au>; s47E(c), s47F @health.gov.au; s47E(c), s47F @Health.gov.au;
 s47E(c), s47F @Health.gov.au; s47E(c), s47F @Health.gov.au
Subject: RE: Response by 13th May: HPRG Intelligence - Nexus Xplore/Onyx FIVECAST Procurement [SEC=OFFICIAL]

Hi s47E(c), s47F

HPRG would need to advise these as part of the procurement process.

I've provided your contact details in the response to the Digital Prioritisation Board, so hopefully they will be in contact.

Regards

Jennifer Frisby (Her/She)

Assistant Secretary
 Health Business Systems Branch | Information Technology Division
 Digital Services within Corporate Operations Group
 Department of Health, Disability and Ageing
 P: 02 5132 s47E(c), s47F IE: Jennifer.Frisby@health.gov.au
 Location: Yaradhang Building
 GPO Box 9848, Canberra ACT 2601, Australia

Supported by Executive Assistant: s47E(c), s47F

This email comes to you from Nggunawal Country. The Department of Health and Aged Care acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

From: s47E(c), s47F @Health.gov.au
Sent: Wednesday, 14 May 2025 8:51 AM
To: FRISBY, Jennifer <Jennifer.FRISBY@Health.gov.au>; Digital Services Prioritisation Board s47E(d) @health.gov.au; CHESHER, Amanda <Amanda.CHESHER@Health.gov.au>
Cc: HOBBSIN, Damien <Damien.HOBBSIN@Health.gov.au>; s47E(c), s47F @health.gov.au; s47E(c), s47F @Health.gov.au;
 s47E(c), s47F @Health.gov.au; s47E(c), s47F @Health.gov.au
Subject: RE: Response by 13th May: HPRG Intelligence - Nexus Xplore/Onyx FIVECAST Procurement [SEC=OFFICIAL]

Good morning all,

I am just finalising the Authority to Proceed. Would someone mind supplying the below detail

Platform for intended implementation: Azure/AWS/GCP

Platform Owner:

System Owner:

Many thanks

Regards,

s47E(c), s47F

Cyber Security Advisor (Contractor)
 Cyber Security Branch | Information Technology Division
 Digital Services within Corporate Operations Group
 Australian Government Department of Health and Aged Care
 T: s47E(c), s47F @health.gov.au
 Location: Yaradhang Level 2 N 8105

From: FRISBY, Jennifer <Jennifer.FRISBY@Health.gov.au>
Sent: Tuesday, 13 May 2025 5:52 PM
To: s47E(c), s47F @Health.gov.au; Digital Services Prioritisation Board s47E(d) @health.gov.au; CHESHER, Amanda

<Amanda.CHESHER@Health.gov.au>

Cc: HOBBLIN, Damien <Damien.HOBBLIN@Health.gov.au>; s47E(c), s47F @health.gov.au>; s47E(c), s47F @Health.gov.au>; s47E(c), s47F @Health.gov.au>; s47E(c), s47F @Health.gov.au>
Subject: RE: Response by 13th May: HPRG Intelligence - Nexus Xplore/Onyx FIVECAST Procurement [SEC=OFFICIAL]

Apologies - Updated to include additional Cyber Security Architecture advice from s47E(c), s47F

Jennifer Frisby (Her/She)

Assistant Secretary
 Health Business Systems Branch | Information Technology Division
 Digital Services within Corporate Operations Group
 Department of Health, Disability and Ageing

P: 02 5132 s47E(c), s47F IE: Jennifer.Frisby@health.gov.au
 Location: Yaradhang Building
 GPO Box 9848, Canberra ACT 2601, Australia

Supported by Executive Assistant: s47E(c), s47F

This email comes to you from Nggunawal Country. The Department of Health and Aged Care acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

From: FRISBY, Jennifer

Sent: Tuesday, 13 May 2025 5:48 PM

To: s47E(c), s47F @Health.gov.au>; Digital Services Prioritisation Board s47E(d) @health.gov.au>; CHESHER, Amanda

<Amanda.CHESHER@Health.gov.au>

Cc: HOBBLIN, Damien <Damien.HOBBLIN@Health.gov.au>; s47E(c), s47F @health.gov.au>; s47E(c), s47F @Health.gov.au>; s47E(c), s47F @Health.gov.au>

Subject: FW: Response by 13th May: HPRG Intelligence - Nexus Xplore/Onyx FIVECAST Procurement [SEC=OFFICIAL]

Hi Digital Services Prioritisation Team,

Thank you for providing the additional information from HPRG on the request. I can see from that further detail, that Chris Bedford (FAS) has reviewed and approved the request as a priority for HPRG. I've still followed up with the HPRG Digital Branch Business Support team who look after HPRG Backlog and prioritisation and they confirmed that it's a known item that they are aware of and are supportive of progressing.

Digital Services contacts have reviewed the request and advised:

- Initial engagement was made in regard to POCs for this initiative back in August 2024. If this is now progressing to procurement and implementation, further additional Cyber assessments are required, on how the products fit into the environment. As an Online top, this should be able to be assessed at pace and an Authority to Proceed provided. The Cyber contact is s47E(c), s47F for preliminary evaluation. We should request as part of the Digital Services response that HPRG reaches out to Cyber as part of the procurement process to allow this Cyber assessment.

Initial findings from Cyber Security Architecture:

- Reviewed and support the HPRG Intelligence procurement
- No OSINT platforms used by Cyber- so no cyber tech capability duplication concern.
- Security platform blueprint includes cyber forensic and threat intelligence capabilities but does NOT include Fraud and Intelligence target state capabilities.
 - Enterprise Architecture to review and advise platform blueprint coverage of Fraud and Intelligence capabilities (Open-Source Intelligence platforms)
- Fivecast Onyx and NexusXplore+ are dominant OSINT platforms
 - Fivecast Onyx has broad FedGov adoption s22
 - NexusXplore+ implemented in s22
- The procurement, commercials, and software management teams have looked at this and have not identified in our scope, that this already exists, so this would be a new procurement. The IT procurement team should remain engaged on this request. Would be good to know how the software is licenced and what opportunities for reuse outside of HPRG there would be.
- From a Data perspective it would need to be confirmed whether data from this software will be stored, and if so where? E.g. It could be combined into the EDAP instance. The contacts for this would be the DAPS branch through their Engage with DAPS process and s47E(c), s47F
- No impact or support would be required from Health Business Systems on this request.

@CHESHER, Amanda – Do you have any architectural considerations that need to be added to the above.

Based on the above, unless Architecture has further concerns, and the contacts above engaged then I'd suggest they could proceed.

If you require further information to provide a response to HPRG, please let me know.

Regards

Jennifer Frisby (Her/She)

Assistant Secretary
 Health Business Systems Branch | Information Technology Division
 Digital Services within Corporate Operations Group
 Australian Government Department of Health and Aged Care

P: 02 5132 s47E(c), s47F IE: Jennifer.Frisby@health.gov.au
 Location: Yaradhang Building
 GPO Box 9848, Canberra ACT 2601, Australia

Supported by Executive Assistant s47E(c), s47F

This email comes to you from Nggunawal Country. The Department of Health and Aged Care acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

From: FRISBY, Jennifer <Jennifer.FRISBY@Health.gov.au>

Sent: Thursday, 8 May 2025 2:20 PM

To: HOBBLIN, Damien <Damien.HOBBLIN@Health.gov.au>; s47E(c), s47F @health.gov.au>; s47E(c), s47F @Health.gov.au>

Cc: Digital Services Prioritisation Board **S47E(d)** [@health.gov.au](mailto:health.gov.au); **S47E(c), S47F** [@Health.gov.au](mailto:Health.gov.au); FRISBY, Jennifer
<Jennifer.FRISBY@Health.gov.au>

Subject: Response by 13th May: HPRG Intelligence - Nexus Xplore/Onyx FIVECAST Procurement [SEC=OFFICIAL]

Hi Damien,

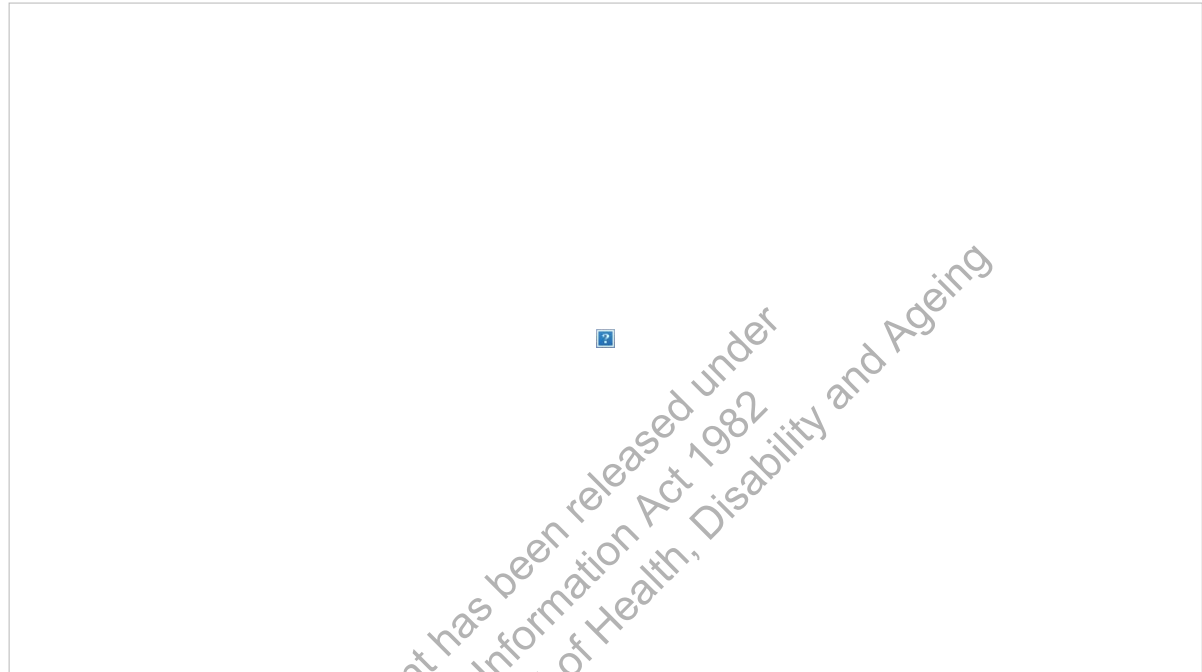
As per the Digital Services Prioritisation Board this morning, can you please provide advice on any concerns/considerations regarding the below request from a Data perspective.

You'd mentioned there was similar in HERD etc, is that the same software or another option?

S47E(c), S47F This is noted as a procurement, do we already have this available in the Department?

S47E(c), S47F Any concerns from Cyber with the sharing of information into this tool (this has been assessed as low risk from a Cyber perspective in the template below – was that assessment in consultation with your team).

If you can please provide a response by **COB Tuesday 13th May**, it would be greatly appreciated.



Regards

Jennifer Frisby (Her/She)

Assistant Secretary
Health Business Systems Branch | Information Technology Division
Digital Services within Corporate Operations Group
Australian Government Department of Health and Aged Care
P: 02 5132 **S47E(c), S47F** | E: Jennifer.Frisby@health.gov.au
Location: Yaradhang Building
GPO Box 9848, Canberra ACT 2601, Australia

Supported by Executive Assistant: **S47E(c), S47F**

This email comes to you from Ngunnawal Country. The Department of Health and Aged Care acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

From: [OSINT tech and tools support](#)
To: [TEPPER, Lisa](#)
Cc: [FLEVARAS, Fay](#); [LUTTON, Tracey](#); s47E(c), s47F ; [IT Business Engagement](#); [Cyber Security](#); [Commercial Software](#); s47E(c), ; [OSINT tech and tools support](#)
Subject: URGENT: Out-of-Session Approval Request for 8 May 2025 Item 7 - FIVECAST Onyx / Nexus Xplore Procurement [SEC=OFFICIAL]
Date: Friday, 20 June 2025 5:22:05 PM
Attachments: [image001.png](#)
Importance: High

Dear Lisa

Issue

We are requesting an urgent out-of-session approval for procurement of Open Source Intelligence (OSINT) software before the end of Financial Year (FY).

Background

1. On 8 May the Digital Services Prioritisation Board met to approve the procurement of OSINT software, however determined that item number 7 required further actions.
 - a. A search was performed to ensure there were not already existing like for like products.
 - b. We have received Authority to Proceed from Cyber Security as well as approval from Enterprise Architecture.

Please be advised there are no outstanding actions remaining.

We have funding set aside specifically for procurement of these tools in this FY. If we do not secure these products this FY, we will lose the funding.

Urgency: s47E(d)

Recommendation

Recommend you approve an urgent out of session meeting.

Thank you.

Kindest regards,

s47E(c), s47F

Assistant Director – Governance, Integrity and Targeted Compliance
Regulatory Compliance Branch

Regulatory Practice and Support Division | Health Products Regulation Group
Australian Government Department of Health, Disability and Ageing

T: 02 5132 s47E(c), s47F [@health.gov.au](mailto:s47E(c), s47F@health.gov.au)

This email comes to you from Ngunnawal Country

Location: Level 2, 27 Scherger Drive, Fairbairn ACT

PO Box 100, Woden ACT 2606, AUSTRALIA

The Department of Health, Disability and Ageing acknowledges First Nations peoples as

the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

From: OSINT tech and tools support

Sent: Thursday, 19 June 2025 11:00 AM

To: Commercial Software s47E(d) @health.gov.au>; s47E(c), s47F

@health.gov.au>; s47E(c), s47F @Health.gov.au>

Cc: s47E(c), s47F @health.gov.au>; IT Business Engagement

s47E(d) @health.gov.au>; s47E(c), s47F @health.gov.au>;

s47E(c), s47F @Health.gov.au>; s47E(c), s47F

@Health.gov.au>; s47E(c), s47F @Health.gov.au>;

LUTTON, Tracey <Tracey.Lutton@health.gov.au>; OSINT tech and tools support

s47E(d) @health.gov.au>

Subject: RE: UPDATE: HPRG Intelligence - FIVECAST Onyx / Nexus Xplore Procurement

[SEC=OFFICIAL]

Importance: High

Hi s47E(c), s47F

Thank you for your call yesterday. Please find below the information you requested.

The intelligence team requires Fivecast Onyx and OSINTCombine's Nexus Xplore by the end of Financial Year (FY) due to operational requirements. These tools greatly increase the capability of the intelligence team, with stakeholders expecting to be able to utilise these capabilities from the end of June. The team has already indicated they will be able to assist with ongoing investigations in multiple branches, s47E(d)

. This support relies on the use of Nexus Xplore and Onyx and, as it relates to current investigations, s47E(d)

Please note how our funding works, if we do not secure these products before end of FY, we will not have the money for our next budget. This may be different with how other branches operate across the department, but not for RCB/VIEB.

Details as requested:

- RCB Financial Business Partner (FBP) – s47E(c), s47F
@Health.gov.au)
- Cost Code – s47E(d)
- We wish to purchase the following number of licences:
 - s47E(d)
 - s47E(d)
- Cost (quote in TRIM links below) estimates.
 - Nexus Xplore Quote - [D25-2164284](#) (Attached)

FIVECAST Onyx Quote – D25-2631485 (Attached)

- Other resources - [E24-458347](#)
-

Vendor Contacts

FIVESCASC

s47F [@fivecast.com](#)

s47F [@fivecast.com](#)

NEXUS

s47F [@osintcombine.com](#)

Thank you.

Kindest regards,

s47E(c), s47F

Assistant Director – Governance, Integrity and Targeted Compliance
Regulatory Compliance Branch

Regulatory Practice and Support Division | Health Products Regulation Group
Australian Government Department of Health, Disability and Ageing

T: 02 5132 s47E(c), s47F [@health.gov.au](#)

This email comes to you from Ngunnawal Country
Location: Level 2, 27 Scherger Drive, Fairbairn ACT
PO Box 100, Woden ACT 2606, AUSTRALIA

The Department of Health, Disability and Ageing acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

From: OSINT tech and tools support

Sent: Wednesday, 18 June 2025 1:38 PM

To: Commercial Software s47E(d) [@health.gov.au](#); s47E(c), s47F

[@health.gov.au](#); s47E(c), s47F [@Health.gov.au](#)>

Cc: s47E(c), s47F [@health.gov.au](#); IT Business Engagement

s47E(d) [@health.gov.au](#); s47E(c), s47F [@health.gov.au](#);

s47E(c), s47F [@Health.gov.au](#); s47E(c), s47F

[@Health.gov.au](#); s47E(c), s47F [@Health.gov.au](#)>

Subject: RE: UPDATE: HPRG Intelligence - FIVECAST Onyx / Nexus Xplore Procurement
[SEC=OFFICIAL]

Importance: High

Hi s47E(c),
s47F

Thank you for reaching out late last week to apprise me of the situation regarding the potential procurement delay of FIVESCASC Onyx / Nexus Xplore.

s22

Thank you.

Kindest regards,

s47E(c), s47F

Assistant Director – Governance, Integrity and Targeted Compliance
Regulatory Compliance Branch

Regulatory Practice and Support Division | Health Products Regulation Group
Australian Government Department of Health, Disability and Ageing

T: 02 5132 s47E(c), s47F @health.gov.au

This email comes to you from Ngunnawal Country

Location: Level 2, 27 Scherger Drive, Fairbairn ACT

PO Box 100, Woden ACT 2606, AUSTRALIA

The Department of Health, Disability and Ageing acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

From: OSINT tech and tools support

Sent: Friday, 6 June 2025 8:24 AM

To: Commercial Software s47E(d) @health.gov.au; s47E(c), s47F

@health.gov.au; s47E(c), s47F @Health.gov.au>

Cc: s47E(c), s47F @health.gov.au; IT Business Engagement

s47E(d) [redacted]@health.gov.au>; s47E(c), s47F [redacted]@health.gov.au>;
 s47E(c), s47F [redacted]@Health.gov.au>; OSINT tech and tools support
 s47E(d) [redacted]@health.gov.au>

Subject: RE: UPDATE: HPRG Intelligence - FIVECAST Onyx / Nexus Xplore Procurement
 [SEC=OFFICIAL]

Good morning s47E(c), s47F [redacted],

s22

Please let us know if you can't find any documentation or if you require any further assistance.

Thank you.

Kindest regards,

s47E(c), s47F [redacted]

Assistant Director – Governance, Integrity and Targeted Compliance
 Regulatory Compliance Branch

Regulatory Practice and Support Division | Health Products Regulation Group
 Australian Government Department of Health, Disability and Ageing
 T: 02 5132 s47E(c), s47F [redacted]@health.gov.au

This email comes to you from Ngunnawal Country
 Location: Level 2, 27 Scherger Drive, Fairbairn ACT
 PO Box 100, Woden ACT 2606, AUSTRALIA

The Department of Health, Disability and Ageing acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders

both past and present.

From: OSINT tech and tools support

Sent: Thursday, 29 May 2025 2:39 PM

To: s47E(c), s47F [redacted] @health.gov.au>

Cc: Commercial Software s47E(d) [redacted] @health.gov.au>; s47E(c), s47F [redacted] @health.gov.au>; s47E(c), s47F [redacted] @Health.gov.au>; OSINT tech and tools support s47E(d) [redacted] @health.gov.au>

Subject: UPDATE: HPRG Intelligence - FIVECAST Onyx / Nexus Xplore Procurement [SEC=OFFICIAL]

Good afternoon s47E(c), s47F [redacted]

I hope this finds you well. By way of introduction, I am from the Regulatory Compliance Branch (RCB) and we have been in discussion with Cyber Security, IT Architecture and s47E(c), s47F [redacted] (previously) from IT Business Engagement regarding the next steps and progression of the approved HPRG Intelligence – FIVECAST Onyx / Nexus Xplore products for procurement.

I have just submitted a new non-standard software request via My Self-Service Portal that has been approved and here is the ticket - **4019938**

Note: My director s47E(c), s47F [redacted] has also confirmed we would like to ensure we can procure these products before the end of this Financial Year (FY) as a bulk payment, as we have specifically set aside funds for this to be allocated this FY.

Please find below the TRIM container that has some pricing estimates:

TECHNOLOGY & TELECOMMUNICATIONS - Evaluation - Regulatory Compliance Branch (RCB) - Opensource Intelligence (OSINT) Tools - [E25-198508](#)

Please let us know if you or the procurement team can't find any documentation or if you require any further assistance.

Thanks s47E(c), s47F [redacted]

Kindest regards,

s47E(c), s47F [redacted]

Assistant Director – Governance, Integrity and Targeted Compliance
Regulatory Compliance Branch

Regulatory Practice and Support Division | Health Products Regulation Group
Australian Government Department of Health, Disability and Ageing

T: 02 5132 s47E(c), s47F [redacted] @health.gov.au

This email comes to you from Ngannawal Country
Location: Level 2, 27 Scherger Drive, Fairbairn ACT

PO Box 100, Woden ACT 2606, AUSTRALIA

The Department of Health, Disability and Ageing acknowledges First Nations peoples as the Traditional Owners of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to all Elders both past and present.

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing



Australian Government

Department of Health, Disability and Ageing

OFFICIAL

ICT Acceptable Use Policy

Direction and guidance for department staff on the acceptable use of departmental Information Communication and Technology assets

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

Contents

Contents	2
1. Introduction	3
2. Purpose	3
3. Responsibilities	3
3.1 Staff	3
3.2 Managers	4
4. Appropriate use	5
4.2 Bring your own device (BYOD)	5
5. Inappropriate use	5
6. Monitoring and auditing of ICT resources	9
6.2 Why monitoring is performed	9
7. Personal information	9
8. Adherence and escalations	10
9. More information	10
9.2 Definitions	10
10. Document information	12
10.1 Version history	12
10.2 Reviewed by	12
10.3 Formal endorsement	13

1. Introduction

- 1.1.1 This ICT Acceptable Use Policy (policy) sets out the expected behaviours when using the Department of Health, Disability and Ageing (department) devices, software, and other services or facilities provided or managed by the department for processing, storing, and communicating information (i.e., ICT resources).
- 1.1.2 This policy is issued for the purpose of subsection 13(5) of the Public Service Act 1999. Your responsibilities under this policy are lawful directions that all staff must adhere to. Non-adherence with your responsibilities detailed in this policy may constitute a breach of the APS Code of Conduct or contract terms, and sanctions may be applied.
- 1.1.3 This policy applies to all staff which includes all Health Australian Public Service (APS) employees, contractors, external service providers, visitors, and other entities who have access to the department's information and ICT resources (including portable ICT equipment).

2. Purpose

- 2.1.1 The primary aim of the department's ICT resources is to support the departmental vision of delivering better health and wellbeing for all Australians, now and for future generations ¹.
- 2.1.2 The intent of this policy is to protect the information held by the department and to ensure staff are accountable for the actions they perform on/with the department's information and ICT assets.

3. Responsibilities

3.1 Staff

- 3.1.1 All staff, as defined in 1.1.3 must:
 - comply with the terms of this policy, to gain and maintain access to the department's ICT resources
 - store corporate information in approved applications such as, and not limited to, s47E(d)
[REDACTED]
 - apply appropriate information classifications labels to all departmental information as detailed in the [Information Security Policy](#)
 - apply appropriate access controls for sensitive and classified information to limit the information to those with a need-to-know² and who hold an appropriate Australian Government Security Vetting Agency (AGSVA) security clearance

s47E(d)

[REDACTED]

- access sensitive and classified information on a need-to-know basis, use client data and personal information consistent with the [Australian Privacy Principles](#)³
- lock or log out of any device used to access the department's information when not in use
- ensure devices are secured at all times. If you lose or misplace your device, report the issue to the Service Desk as soon as possible
- never share user credentials and/or passwords/passphrases with any other person
- never request another user's credentials and/or passwords/passphrases
- never interfere or attempt to interfere with security and/or access control measures
- not operate unapproved software or hardware on departmentally managed devices systems
- not elevate their own system accesses or grant additional access to their own accounts
- grant access to systems, only with the appropriate approval, and remove access when no longer required for themselves and other staff
- ensure access to ICT resources is limited to the minimum permissions needed to perform the required role or approved business function
- any documentation, decisions or business communications must be captured as records in the approved system, such as, but not limited to §47E(d) including on BYOD.
- accept that actions carried out on the department's ICT resources, such as managed devices, are subject to monitoring and auditing
- report suspected or actual breaches of this policy, and any cyber security incidents to the Cyber Security Branch via the [cyber security incident reporting form](#).

3.2 Managers

3.2.1 In addition to the responsibilities of staff, a manager must also:

- ensure staff hold the appropriate AGSVA security clearance and have undergone pre-employment checks to access the department's resources
- ensure staff understand and comply with this policy
- ensure staff complete all mandatory training
- ensure exit procedures are performed for staff leaving the department
- ensure staff access to ICT resources is removed in a timely manner when it is no longer required (e.g. changing roles)
- ensure staff exiting the department return all department ICT assets on their final day of work as per the [Resignation Policy](#).
- refer suspected unlawful, unreasonable, or unethical access and/or behaviours to the [People Management Section](#)
- refer suspected fraudulent or corrupt use of the department's ICT assets via the [Report fraud and corruption](#) mechanisms.
- Report suspected data breaches involving ICT resources to the Privacy Law Section, in accordance with the department's data breach response plan: [Data breach response plan.pdf \(sharepoint.com\)](#)

4. Appropriate use

4.1.1 The department provides ICT resources to support the objectives of the department. Limited personal use is permitted as outlined in this policy. At all times when using the department's ICT resources, including managed devices, you should consider:

- if your usage is lawful
- if your usage is consistent with the APS Code of Conduct⁴.
- if your usage interferes with the work obligations of you and/or colleagues
- if your usage could damage the integrity and/or reputation of the Commonwealth, the department, or colleagues.

4.2 Bring your own device (BYOD)

4.2.1 The department provides an opt-in mobile device management solution, known as BYOD, to enable staff to use their own personal device to access selected corporate services and information.

4.2.2 To access this service, staff must read and agree to this ICT Acceptable Use Policy, and the BYOD End User Agreement.

5. Inappropriate use

Use of the department's ICT resources must align to the Public Service Act, APS Values, APS Code of Conduct, and, the Department's values.

Use of the department's ICT resources must not at any time be unlawful, inappropriate, or unacceptable including (but not limited to):

- fraud
- defamatory conduct
- harassment and/or bullying (direct or indirect)
- using language that may be seen as inappropriate, offensive, or unacceptable
- stalking and/or privacy violations
- excessive non-work-related communication or internet use.

5.1 Illicit material

Staff must not display, download, create, distribute, publish, copy, and/or store illegal or offensive material or links to offensive material on departmentally issued mobile devices including, but not limited to:

- pirated or unauthorised copyright material
- material containing discriminatory content
- pornography and/or offensive content
- material that contains offensive, abusive, harassing, discriminatory, vilifying, or defamatory language
- material that a reasonable person might consider inappropriate, objectionable,

or offensive in a work environment.

5.2 Unacceptable Use

5.2.1 Use of departmentally issued ICT resources, including mobile devices, by staff must not constitute unacceptable or inappropriate actions including, but not limited to:

- conducting business activity for private commercial or profit making
- trading shares and/or gambling
- seeking commercial gain from the department's information
- political or social campaigning
- unauthorised comments on government policy (including comments that could be considered non-apolitical)
- using dating sites, unapproved instant messaging, or chat room services
- accessing or sharing information without a need-to-know
- Sharing, downloading or streaming files or content is prohibited unless required for legitimate business purposes and undertaken in accordance with departmental ICT policies and approvals.
- using unapproved web-based email services
- discrediting other individuals, the department, or the Government.

5.3 Compromising security

5.3.1 Use of departmentally issued ICT resources, including mobile devices, by staff must not compromise the security of department including, but not limited to:

- connecting unauthorised devices to the department's network
- accessing ICT resources using unapproved hardware
- purposely gaining or attempting to gain unauthorised access to data, other user's data, or departmental resources and/ or systems
- performing unauthorised actions on the department's resources or systems
- providing any unauthorised individual access to the department's ICT resources
- sharing credentials, or storing credentials in an insecure manner
- downloading or installing applications not approved for use under the [PSPF](#), including TikTok and DeepSeek. This list may be updated from time to time.
- using unapproved software or online services
- using or storing departmental material and or information on unapproved file sharing or cloud services
- purchasing and/or using cloud services not approved for use
- attempting to bypass relevant internet content filters
- unauthorised disclosure or mishandling of personal or sensitive and classified information
- purposely renaming or masking electronic materials to hide true contents
- connecting to vehicle infotainment systems, allowing connected vehicles to access, synchronise, copy or store information from departmentally issued devices, or personal

devices containing departmental information.

5.3.2 Staff must not disclose or access (deliberately or inadvertently):

- personal, sensitive, or classified information to any party that does not have a need-to-know
- information to gain or seek to gain a benefit or advantage for private commercial or profit making
- information to cause or seek to cause detriment to the Department, Commonwealth, or any other person.

5.4 Email usage

5.4.1 Use of the department's email services by staff must not compromise the security of the department's information, resources, and reputation, including:

- using departmental email addresses when signing up for any kind of public accounts, on any social media platforms, unless required as part of work duties
- sending work related and/or sensitive or classified emails and attachments to personal email addresses
- sending mass distribution messages, including spam, 'not-for-profit' messages, chain letters or hoax emails
- using Inbox rules to forward email to an external email address not listed in the department's Global Address Book.

Emails must be secured, and protective markings must be applied to emails to reflect the highest sensitivity or classification of the subject, body, and attachments, in accordance with the departments [Information Security Policy](#).

5.5 Use of generative AI tools

The department is implementing [whole-of-government guidance](#) on artificial intelligence (AI) and continues to update internal policies accordingly in alignment with the department's risk environment.

An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

Generative AI is technology that generates content such as text, images, audio, and code in response to user prompts (such as Copilot, ChatGPT, Claude, Gemini and Grok).

The use of AI, including but not limited to Generative AI, for any work purpose should be guided by departmental policies and guidance, align with approved products, and not allow unauthorised AI tools to access the departmental ICT resources. See [Using AI at work](#) for current guidance.

Approval for new software including AI should be via the IT Business engagement team s47E(d) [@health.gov.au](#)) or via the IT Helpdesk portal.

s47E(d)

s47E(d)

5.7 Private or personal use

The department accepts that employees may use departmentally issued and controlled devices to access ICT resources such as the internet, email, and instant messaging, for limited and occasional personal use.

5.7.1 All use on departmentally issued and controlled devices may be subject to [freedom of information](#) (FOI) requests or assessment by relevant business areas including (but not limited to) Integrity and Assurance, Information Technology and People, Communication and Parliamentary Divisions should the department believe there is a requirement to do so.

5.7.2 Use of the department ICT resources is not consistent with this Policy when it:

- may result in unreasonable cost or performance impacts on the department
- interferes with your work obligations, or those of your colleagues
- falls within the scope of what is considered inappropriate use
- could damage the integrity and good reputation of the department, its employees, clients, or the Commonwealth.

The following are examples of websites considered appropriate for limited and occasional personal use include:

- bank and credit union websites
- insurance and superannuation websites
- telephone directories
- territory, regional, state and Australian Government websites
- child-care centers, schools, and universities
- news and current affairs websites
- search engines.

6. Monitoring and auditing of ICT resources

- 6.1.1 All resources managed and/or procured by the department are subject to ongoing and sustained monitoring and auditing. Data collected through this process includes but is not limited to, whenever a user or device:
- accesses or interacts with a department's resources
 - applications run or fail to run
 - accesses or fails to access, data, files and or email
 - connects to or uses the internet, including site, pages visited, and files downloaded/ uploaded
 - interacts with the network, including Wi-Fi network
 - uses personal devices to connect to or otherwise access the department's ICT resource
 - s47E(d)

6.2 Why monitoring is performed

- 6.2.1 The department performs monitoring and auditing to:
- protect data, assets, property, and finances from unlawful activity
 - protect data, assets, property, and finances from activities in breach of this policy
 - ensure the department's ICT resources are operating in an efficient, effective, ethical, and economical manner.

7. Personal information

- 7.1.1 Your personal information is protected by law, including the Privacy Act 1988 and the Australian Privacy Principles. The department collects personal information relating to personnel for the purpose of monitoring and managing corporate applications and transactions in accordance with this and other policies. This collection of information includes:
- network monitoring and diagnostics
 - mobile device management monitoring
 - internet browsing
 - use of messaging and email services
 - application, file server and other use of department ICT resources.
- 7.1.2 Your personal information that is collected may be used and disclosed to support:
- the delivery of ICT services
 - APS code of conduct and fraud investigations
 - the disclosure of information under or required by a law of the Commonwealth

- FOI requests
- contractual arrangements with service providers
- memoranda of understanding (MOU) arrangements with customer agencies
- investigations by Federal or State police services
- Cyber Security Investigations and Incident responses
- other situations where the CISO or Chief Security Officer (CSO) require access to your information.

7.1.3 Information you provide through your personal use of departmental ICT resources will be collected by the department. Personnel who do not want the department to collect their personal information in connection with their personal use of ICT resources should not use the department's ICT resources for personal transactions.

7.1.4 You can find more information about the way in which the department will manage your personal information, in the [Privacy Policy](#).

7.1.5 Information collected may be disclosed by the department to applicable Commonwealth entities or contracted service providers for the purpose of analysis, auditing, diagnostics, service improvements, reporting and/or to ensure personnel are adhering to this policy.

s47E(d)

8. Adherence and escalations

Failures to adhere to this policy will be managed by the Cyber Security Branch, Integrity and Security Branch, People Branch, and any other relevant bodies in accordance with the departments [Security Incident Management and Reporting Policy](#).

Manager discretion applies when enforcing this policy (i.e. definitions around limited personal use thresholds) and exclusions for legitimate business purposes can be facilitated by the Cyber Security Branch at [s47E\(d\) @health.gov.au](#).

9. More information

9.1.1 For more information contact the Cyber Security Branch at [s47E\(d\) y@health.gov.au](#), related policies are located on the [Security Awareness](#) page.

9.2 Appendix

[What we do | Australian Government Department of Health and Aged Care](#)
[Australian Privacy Principles | OAIC](#)

9.3 Definitions

Clients	Clients are individuals and organisations that apply for funding from department or otherwise use the department's services.
----------------	--

Customers	Customers are organisations, which use the department's resources as a shared service.
ICT resources	Devices, software, and other services or facilities provided by the department for processing, storing, and communicating information.
Need-to-know	The need-to-know principle applies to all personal, sensitive, and classified information. It reflects the need for staff to access this information only where there is an operational requirement to do so. The practice helps staff understand their responsibility to protect information, including the correct methods for storage, handling, and dissemination.
Staff	All individuals who have been provided with access to the department's ICT resources to support official business and its customers.
System	Used for the processing, storage or communication of information and the governance framework in which it operates.
Generative artificial intelligence (AI)	Generative artificial intelligence (AI) is technology that generates content such as text, images, audio, and code in response to user prompts (such as Copilot, ChatGPT, GPT-4, AlphaCode or Bard).
Remote wipe	A function activated by the department to restore the device to factory settings, therefore removing all information from the device.
s47E(d)	
Need-to-know	The need-to-know principle reflects the need for personnel to access this information only where there is an operational requirement to do so.
Infotainment system	An in-vehicle system that provides functions such as navigation, audio, calls, messaging, voice control, device pairing, wireless projection, telematics or application integration.
Connected vehicle	A vehicle with network, wireless, cellular, Bluetooth, Wi-Fi, infotainment, telematics, navigation, voice assistant or similar capability that may collect, store, transmit or synchronise information.

10. Document information

10.1 Version history

The following table shows the version history for this document:

Version	Date	Author(s)	Description of Change
1	11/08/2020	Various	Previous published Version
2	20/1/2024	Cyber Security Branch	Review and update, apply new document template.
2.1	24/11/2024	Cyber Security Branch	Updated with minor feedback and noting CISO approval and NSPF consultation.
2.2	08/08/2025	Information Management Section	Add records created on mobile devices should be saved to s47E(d).
2.3	08/08/2025	Information Management Section	Added records created on mobile devices should be saved to s47E(d).
2.4	09/12/2025	Cyber Security Branch	Updates to BYOD terms and conditions, s47E(d) and policy adherence.
2.5	24/02/2026	Cyber Security Branch	Updates to BYOD terms and conditions.
3.0	TBD		Final for release

10.2 Reviewed by

The following table lists the reviewers for this document:

Name	Role	Group/Organisation	Date
s47E(c), s47F	A/g Director, Cyber Security	COG, ITD	20/03/2024
	Director, Personnel Security	COG, ITD	12/04/2024
	Director, Digital Workspace, and Infrastructure Delivery Executive Director	COG, ITD	30/05/2024
	Information Law Section	COG, LD	09/07/2024
Various	Workplace Relations Section, People Management Section.	COG, PCPD	20/06/2024
Various	National Staff Participation Forum	NSPF	25/10/2024
s47E(c), s47F	A/g Director, Cyber Security	ITD	24/02/2026

10.3 Formal endorsement

The authorisers listed in the endorsement table below acknowledge that this document meets the specified purpose.

Name	Role	Date
Jonathan Leen	A/g Assistant Secretary, Service Operations, and Infrastructure	20/04/2026
Luke Johnson	Assistant Secretary and Chief Information Security Officer, Cyber Security	08/05/2026

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

Health.gov.au

All information in this publication is correct as of March 2026

This document has been released under
the Freedom of Information Act 1982
by the Department of Health, Disability and Ageing

OFFICIAL



Australian Government

Department of Health, Disability and Ageing
Therapeutic Goods Administration

Integrity Policy

Regulatory Compliance Branch

Name of procedure/policy	Regulatory Compliance Branch Integrity Policy
Applicable to	Regulatory Compliance Branch and Vaping Implementation and Enforcement Branch
TRIM Ref no	D26-1879796
Document Owner	Targeted Compliance and Regulatory Strategy Section
Authorised	s47E(c), s47F
Approval Date	1 May 2026
Document contact	Targeted Compliance and Regulatory Strategy Section
Written by	s47E(c), s47F
Version no.	3

OFFICIAL

OFFICIAL

Contents

Purpose	3
Responsibility	3
Training essentials	5
Declarations related to conflicts of interest	5
Nothing to declare	5
Conflict to declare	5
Regular re-consideration	6
Warrants	6
Changes in circumstances	6
Outside employment	6
Record Keeping	7
Procedure for Electronic Signing	7
Resources	7
Version history	8
Flow chart	9

OFFICIAL

OFFICIAL

Purpose

This policy sets minimum requirements for all Regulatory Compliance Branch (RCB) staff¹.

The Department of Health, Disability and Ageing (the Department) maintains a [Conflict of Interest Policy](#) that describes when employees must declare a conflict of interest. This policy document specifies additional expectations for Regulatory Compliance Branch (RCB) staff to regularly re-consider conflicts of interest, and for RCB to keep centralised records of these re-considerations.

Responsibility

The Targeted Compliance and Regulatory Strategy (TCRS) Section in RCB maintains this document and the centralised record-keeping for Conflicts of Interest (COI) declarations by RCB staff.

Directors, with support from TCRS, are responsible for ensuring staff of their sections:

- Maintain their essential training as required in SuccessFactors;
- Consider conflicts of interest upon commencement for new staff;
- Re-consider their conflicts of interest regularly; and
- Provide the Governance team with updated information to maintain the staff register.

Role	Description
Governance Team	Monitor Essential Learning Program modules. Maintain centralised record-keeping for COI declarations. Conduct an annual COI review and request that all staff re-consider and complete an annual declaration in March of each year.

¹ In November 2023, the Vaping Implementation and Engagement Branch was established to, in part, conduct nicotine vaping product investigations for the TGA. For the purposes of this document, references to RCB will mean the Regulatory Compliance Branch and the Vaping Implementation and Engagement Branch.

OFFICIAL

OFFICIAL

Role	Description
Directors	Ensure staff in their sections meet their essential learning training obligations. Note: You can view percentage completion by classification and by module and download of list of those who haven't completed their modules in excel format via MyWorkforce reporting tool. Must ensure that a COI declaration has been completed within the first week of commencement of new staff. Ensure staff in their section regularly review and reconsider their COI declarations and complete their essential learning refresher training. Must notify the Governance team of new staff starting in their section. Advise the Governance team of a staff member/s final working day at least 1 week in advance. Note: Staff involved in investigations are expected to provide personal contact details in the event they are required to give evidence in relation to their role in an investigation.
AS	Review and approve COI management plans.
All RCB Staff	Must complete their COI and essential learning within the first week of commencing with RCB. Regularly review and reconsider their COI declarations and complete their essential learning refresher training. Immediately complete and submit a new COI declaration when their circumstances change, rather than waiting for the annual COI process. Complete a new COI if attending a warrant (including warrant assists with other agencies and friendly or cooperative warrants). Note: Staff involved in investigations are expected to provide personal contact details in the event they are required to give evidence in relation to their role in an investigation.

OFFICIAL

OFFICIAL

Training essentials

The Department provides ongoing training to ensure staff know their minimum obligations for critical integrity related areas, such as fraud, security and privacy. Directors are responsible for ensuring their staff complete all essential training within the first week of the staff member receiving access to SuccessFactors².

Where an RCB staff member is on extended leave over the due date, the Director will ensure the training is completed within 1 week of the staff member's return to work.

TCRS will conduct regular checks on Essential Learning modules completed by RCB personnel.

Where it is identified that RCB personnel still need to complete or maintain their essential learning, the TCRS section will work with the relevant personnel and their manager/Director to ensure the required actions are undertaken.

Declarations related to conflicts of interest

The [Exit and entry expectations of RCB staff members Policy](#) sets expectations for new staff to make declarations, as per below.

The Department's [Conflict of Interest Policy](#) sets out under what circumstances you must disclose a conflict of interest and how these conflicts are to be managed. Any real, apparent or potential conflicts of interest should be dealt with according to this policy.

The TCRS section will maintain a register of when RCB staff members have most recently made declarations.

The TCRS section will issue annual requests (March or as close to) for staff to complete Conflict of Interest (COI) declarations. All staff are expected to regularly reconsider their declarations on an ongoing basis. The annual request is a minimum assurance activity and does not replace a staff member's obligation to submit a new COI declaration when circumstances change during the year.

Important: The 12-month annual COI process is not a waiting period. If your circumstances change, you must complete a new COI declaration at that time.

Nothing to declare

If an RCB staff member considers that they have nothing to declare, that staff member is to prepare an [Declaration of Interests Form \(Nothing to declare\)](#) and submit to their Director for consideration. If the Director considers that the staff member has appropriately considered the potential for conflicts of interest, the Director should confirm the form prepared by their staff member. The form and electronic signatures should be recorded as per [Procedure for Electronic Signing](#) and the TCRS section notified to update the staff register.

Conflict to declare

If an RCB staff member suspects they have or it would be reasonable for others to perceive they have a conflict of interest, that staff member is to complete a [Declaration of Interests Form](#) and submit to their Director for consideration. Staff should discuss the completed form with their manager. It must then be forwarded to the relevant Assistant Secretary (or higher, if appropriate) for review and approval of the proposed management plan. Once the

² There are commonly delays in new staff receiving access to SuccessFactors.

OFFICIAL

OFFICIAL

employee, the Director and the AS, has signed the form, it should be provided to HR, saved in TRIM and TCRS notified to update the staff register.

Regular re-consideration

At least once per calendar year, TCRS will advise section Directors of staff who have yet to update or confirm their declarations in the previous 12 months. RCB staff are expected to submit and provide a new declaration. This annual process does not remove the requirement to submit a new COI declaration immediately if a staff member's circumstances change at any time during the year.

Directors are to ensure declarations/confirmations are managed appropriately and relayed to TCRS within 1 week of this advice.

Note: *If a declaration has already been completed by an employee 3 months prior to an annual declaration request, another declaration is not needed. However, in keeping with departmental policy, all staff must regularly re-consider their existing declarations.*

Warrants

Staff participating in warrants must complete an additional COI form before each warrant.

Staff participating in, supporting, or otherwise involved in warrant activity must complete an additional COI form prior to each warrant.

This requirement applies to warrants led by the Regulatory Compliance Branch, warrant assists conducted with other Commonwealth, state or territory agencies, and "friendly" or cooperative warrants, including where RCB staff attend in an observer, advisory, specialist, or support capacity.

To ensure the warrant holder can appropriately manage any conflicts, staff should sign declarations after the warrant pre-briefing but before they travel to the warrant. Additional declarations should be saved in TRIM in the relevant investigation folder and TCRS notified to update the staff register.

Note: *For the purposes of this policy, attendance at a warrant includes operational participation, observational attendance, technical or specialist support, advisory roles, and any other involvement where the staff member is present as part of warrant activity.*

Changes in circumstances

Staff must complete and submit a new Conflict of Interest (COI) declaration as soon as practicable when their circumstances change.

This requirement applies regardless of when the staff member last completed an annual or other COI declaration. Staff must not wait for the annual COI process or the 12-month review cycle if a change occurs.

Changes in circumstances include, but are not limited to:

- commencement, cessation, or change in secondary employment
- membership of clubs, associations, boards, or committees
- volunteering activities
- changes to personal, financial, or professional relationships; or
- any other situation that could give rise to a real, potential, or perceived conflict of interest.

Outside employment

When completing an [Outside Employment Form](#), staff should complete a new declaration of interest. The new declaration should reference the outside employment to indicate that the

OFFICIAL

OFFICIAL

staff member has considered the outside employment and any associated real or perceived conflicts.

Record Keeping

Directors should ensure required records of declarations (and associated paperwork) are maintained in TRIM folders identified for this purpose by TCRS; and advise TCRS when new declarations have been managed and associated documentation filed.

Procedure for Electronic Signing

1. Save a copy of the relevant Declaration of Interests Form ([Declaration of Interests Form \(Nothing to declare\)](#)) and name the document "Annual Conflict of Interest Declaration Form – First and Last Name – YYYY".
2. Electronically fill in your name and the date. In the signature field add "Signed electronically in TRIM".
3. In TRIM, assign the **Signature** workflow and add yourself as the Responsible Location, using the instructions to "Assign a Single Action" found at [TRIM Help Card - Workflow - Assign Actions](#).
4. Complete the workflow and finalise the document using the instructions "Complete an Action" found at [TRIM Help Card - Complete or reject an Action](#).
5. After completing the action, repeat step 3 and assign the next **Signature** workflow to your Director as the Responsible Location, using the instructions to "Assign a Single Action" found at [TRIM Help Card - Workflow - Assign Actions](#).
6. File the completed declaration in the relevant section TRIM container.

Note: The TRIM containers have access restrictions in place, please ensure you and your director have both co-signed the declaration prior to saving it into the relevant section TRIM container established by TCRS.

Resources

[Declaration of Interests Form](#)

[Declaration of Interests Form - Nothing to declare](#)

[Department of Health Conflict of Interest Policy](#)

[Department of Health Outside Employment Policy](#)

[Exit and entry expectations of RCB staff members Policy](#)

OFFICIAL

OFFICIAL

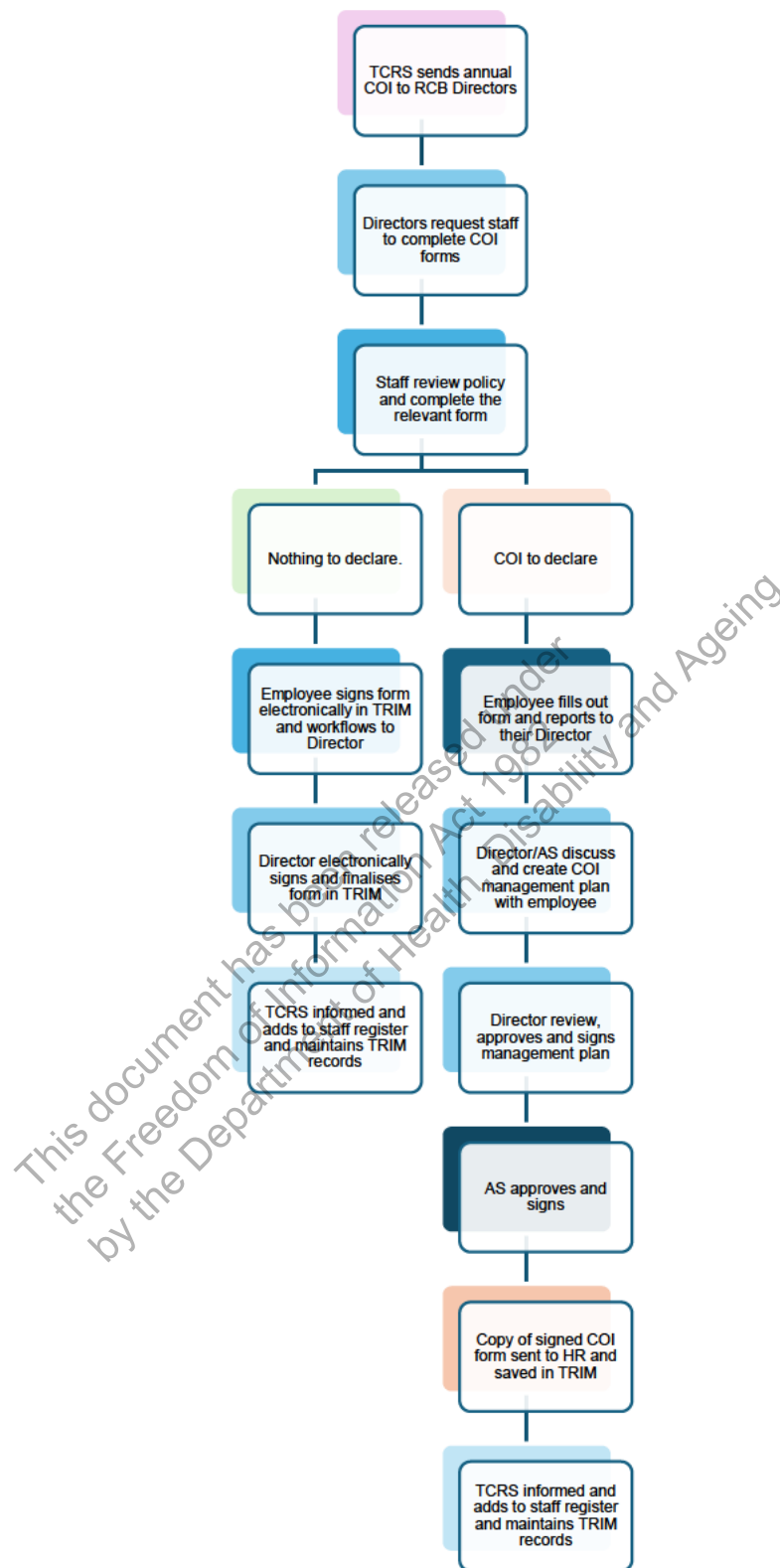
Version history

Version	TRIM Reference	Description of change	Author/s	Effective date	Review Date
V0	D24-2943325	Original SOP	s47E(c), s47F	7/06/2024	7/06/2025
V1	D25-1228578	Annual review and update		17/09/2025	17/09/2026
V2	D26-1028849	Clarified Conflict of Interest requirements for warrant activity, including warrant assists and friendly or cooperative warrants. Adjusted the timeframe to ensure Conflict of Interest declarations and Essential Learning are completed during the first week of branch commencement.		03/03/2026	03/03/2027
V3		Update made to the Regularly Re-consider section (page 3). Removed the highlighted wording to reflect our current expectations <i>RCB staff are expected to submit and provide a new declaration or confirm their existing declaration via email to their Director.'</i>		01/05/2026	01/05/2027

OFFICIAL

OFFICIAL

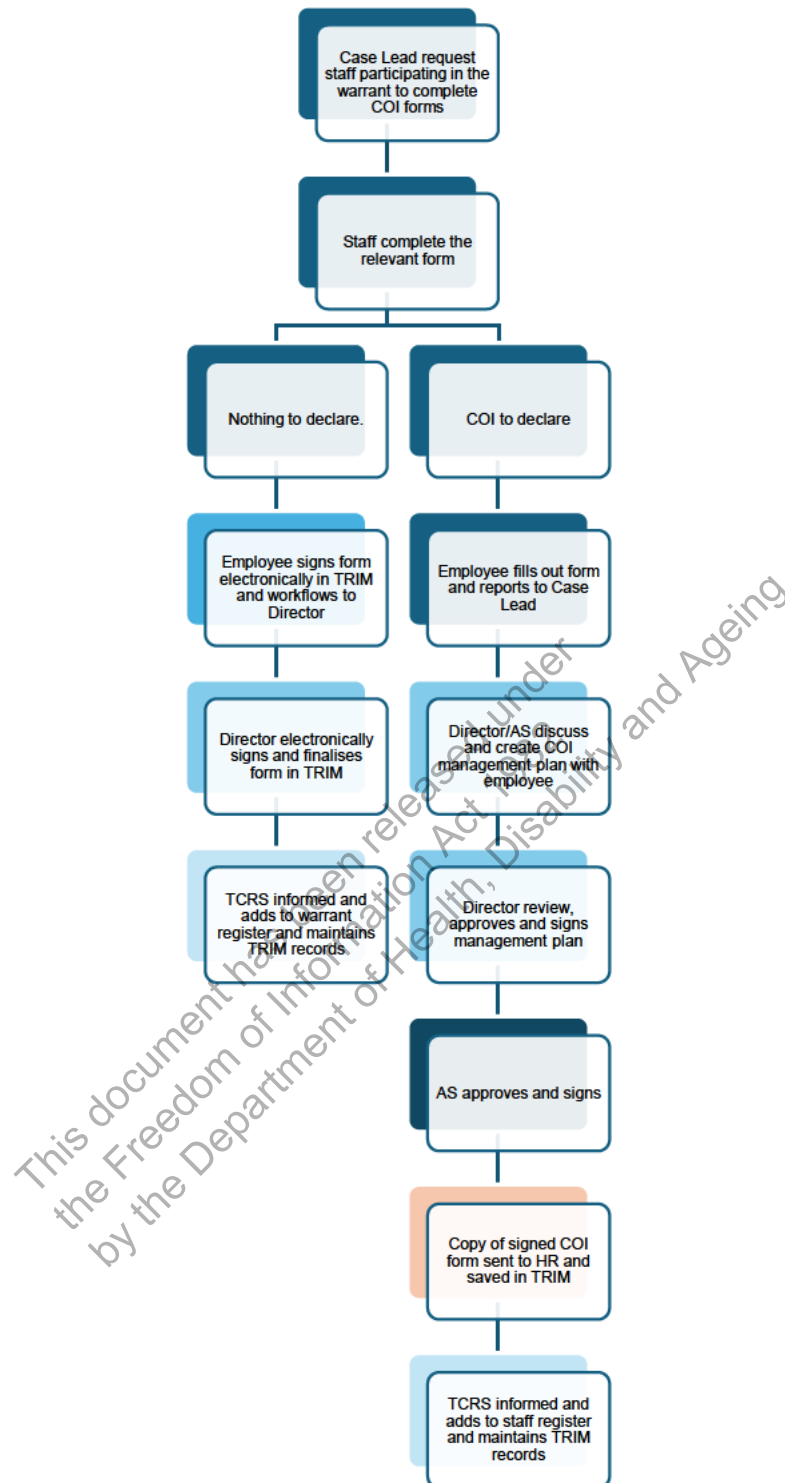
Flow chart – Annual COI



OFFICIAL

OFFICIAL

Flow chart – Warrant COI



OFFICIAL