s22

From: s22 @heidihealth.com>
Sent: Thursday, 24 September 2026 5:50 PM
To: Hickin, Lee
Cc: Conroy, Kate; s22
Subject: Re: Heidi's interest in the AI safeguards working group [SEC=OFFICIAL]

CAUTION - This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Thank you, Lee. I really appreciate you coming back to me on this.

Hope you are well, and please let me know if there is anything we can do to support the Centre and its work.

Kind Regards,
s22

On Thu, 24 Sept 2026 at 16:09, Hickin, Lee s22 @industry.gov.au> wrote:

OFFICIAL

I'm sorry s22 , I don't have a direct contact there. My colleague at the s22 might be able to point you in the right direction.

Kind Regards,

Lee Hickin

National AI Centre Executive Director

Dept. Industry Science and Resources | Head of Division

Phone s22 | **Email** s22 @industry.gov.au

Australian Government | National AI Centre

s22 , Sydney NSW 2000 Australia

Department of Industry, Science and Resources

| Visit AI.gov.au

Subscribe to our newsletter to receive regular updates and all the latest news from the National AI Centre.

Acknowledgement of Country

Our department recognises the First Peoples of this Nation and their ongoing cultural and spiritual connections to the lands, waters, seas, skies, and communities.

We Acknowledge First Nations Peoples as the Traditional Custodians and Lore Keepers of the oldest living culture and pay respects to their Elders past and present. We extend that respect to all First Nations Peoples.



OFFICIAL

From: s22 @heidihealth.com>
Sent: Thursday, 24 September 2026 12:39 PM
To: Hickin, Lee <s22 @industry.gov.au>
Cc: s22 @heidihealth.com>
Subject: Re: Heidi's interest in the AI safeguards working group [SEC=OFFICIAL]

CAUTION - This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Thanks Lee. Do you by any chace know who I can reach out to?

Kind Regards,

s22

On Thu, 24 Sept 2026 at 12:26, Hickin, Lee <s22 @industry.gov.au> wrote:

OFFICIAL

Thank you for reaching out s22 .

The Medicare/OpenAI incident is being handled directly by the National Office for Cyber Security (https://www.nationalcybersecurity.gov.au/) – I would suggest you reach out to them directly with your generous offer to support.

Kind Regards,

Lee Hickin

National AI Centre Executive Director

Dept. Industry Science and Resources | Head of Division

Phone s22 | **Email** s22 @industry.gov.au

Australian Government | National AI Centre

s22 , Sydney NSW 2000 Australia

Department of Industry, Science and Resources

| Visit AI.gov.au

Subscribe to our newsletter to receive regular updates and all the latest news from the National AI Centre.

Acknowledgement of Country

Our department recognises the First Peoples of this Nation and their ongoing cultural and spiritual connections to the lands, waters, seas, skies, and communities.

We Acknowledge First Nations Peoples as the Traditional Custodians and Lore Keepers of the oldest living culture and pay respects to their Elders past and present. We extend that respect to all First Nations Peoples.



OFFICIAL

From: s22 @heidihealth.com>
Sent: Thursday, 24 September 2026 11:19 AM
To: Hickin, Lee <l s22 @industry.gov.au>
Cc: s22 @heidihealth.com>
Subject: Heidi's interest in the AI safeguards working group

CAUTION - This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hi Lee,

I hope you are well. I'm writing on behalf of Heidi following today's news on the OpenAI agent's access to the Medicare Statistics Reporting Service portal.

As you are aware, Heidi is a sovereign AI company. We manage our infrastructure and data onshore, and our security and governance are built for healthcare from the outset.

We would like to be involved in the working group and contribute our experience in this area. We

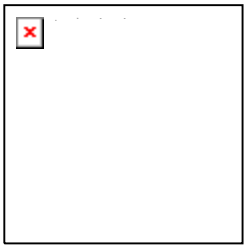
believe local expertise has a role to play in this process.

I am available to discuss this week at your convenience.

Kind Regards,

s22

--

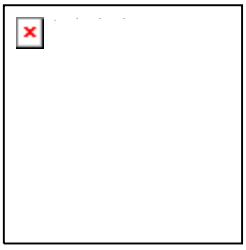


s22

Head of Public Policy

heidihealth.com

--

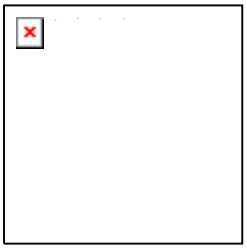


s22

Head of Public Policy

heidihealth.com

--



s22

Head of Public Policy

heidihealth.com

Thursday, 24 September

DISR – for release under the FOI Act Document 2 - FOI 300755

24/09 11:21 am

Hey there - I've had Heidi health reach out wanted to help in the effort to understand and protect against the Medicare incident.....are you (AISI) involved in that and can I point her to you or is there a better point of contact you can suggest ?

Conroy, Kate 24/09 11:29 am

National Office for Cyber Security

24/09 11:30 am

do you have a contact ? thank you

Conroy, Kate 24/09 11:30 am

https://www.nationalcybersecurity.gov.au/

DISR – for release under the FOI Act

Thursday, 24 September

Document 3 - FOI 300755

s22

24/09 8:01 am

s22

FYI: AI agent accessed Australian government site, Anthony Albanese says - ABC News



AI agent accessed Australian go...

Prime Minister Anthony Albanese says an unauthorised AI agent has accessed...

www.abc.net.au

s22

24/09 8:37 am

s22

Concerning stuff... though I've now gotten this from about 5 different directions 😄

24/09 8:38 am

"The company did not notify Services Australia of the incident until three months after the fact, via email." - on some level you have to admire the audacity ! 🙄

Edited

perhaps they spent 3 months trying to figure out if it was Austria or Australia ?

DISR – for release under the FOI Act

Document 4 - FOI 300755

s22 24/09 8:40 am

s22

There's a whole bunch of updates here that resolved questions I had that weren't in the original article. Primarily: that it was initiated out of OpenAI itself, not someone random running OpenAI models

Federal politics live: OpenAI took three months to report Medicare breach, PM says - ABC News



Federal politics live: OpenAI too...
An OpenAI agent has accessed public and private data after hacking into a...
www.abc.net.au

s22 24/09 8:41 am

s22

> s22 24/09/2026 8:37 am
> Concerning stuff... though I've now gotten this from about 5 different directions 😄

is it really concerning?

s22 24/09 8:43 am Edited

s22

I think Marles put it best

> "The information is benign in a sense and as I say, the impact is relatively minor, but the incident is very serious."

s22

From: s22 @cyberalchemist.com.au>
Sent: Thursday, 24 September 2026 10:36 AM
To: Hickin, Lee
Subject: OpenAI/Medicare

Hi Lee,

Putting my hand up if you are in a position to suggest people for the task force. As you know, digital forensics and IRAP have been my things.

Regards,

s22 **| THE CYBER ALCHEMIST PTY LTD**
s22 NSW 2092
E: s22 @cyberalchemist.com.au | M: s22 W: www.cyberalchemist.com.au

s22

From: Wilson, Helen
Sent: Monday, 28 September 2026 10:31 AM
To: Pickworth, Julia; All Industry Division Heads; Executive Board Distribution List - EIA; Laws, Rebecca; Croft, Joanne; O'Sullivan, Sybille; Webb, Alex; Writer, Simon; Smith, Kate
Subject: WoG talking points OpenAI incident [SEC=OFFICIAL]
Attachments: Talking Points - OpenAI cyber incident v3.docx

OFFICIAL

As discussed,

Thanks H

OFFICIAL

-----Original Appointment-----
From: Pickworth, Julia
Sent: Thursday, 21 May 2026 11:42 AM
To: Pickworth, Julia; All Industry Division Heads; Executive Board Distribution List - EIA; Laws, Rebecca; Croft, Joanne; O'Sullivan, Sybille; Webb, Alex; Writer, Simon; Smith, Kate
Subject: 10AM | HoD's and EB meeting [SEC=OFFICIAL]
When: Monday, 28 September 2026 10:00 AM-11:00 AM (UTC+10:00) Canberra, Melbourne, Sydney.
Where: Microsoft Teams Meeting

s 22

s22

Executive Assistant to Julia Pickworth
Department of Industry, Science and Resources
Ngunnawal Country, Industry House, 10 Binara Street (GPO Box 2013) Canberra ACT 2601 Australia
Teams call | s22 @industry.gov.au

I industry.gov.au ABN 74 599 608 295
Supporting economic growth and job creation for all Australians | We are collaborative, innovative, respectful and strive for excellence

Acknowledgement of Country

Our department recognises the First Peoples of this Nation and their ongoing cultural and spiritual connections to the lands, waters, seas, skies, and communities.

We Acknowledge First Nations Peoples as the Traditional Custodians and Lore Keepers of the oldest living culture and pay respects to their Elders past and present. We extend that respect to all First Nations Peoples.

DISR – for release under the FOI Act

Document 7 - FOI 300755

Australian Government
Department of Home Affairs

** OFFICIAL**

TALKING POINTS

Subject	OpenAI incident	
Date	26 September 2026	**Version**: 3
Type	Whole of Government	
Media Officer: s22	**Media Ph:** s22	

ISSUE

Talking points for OpenAI incident

TALKING POINTS OFFICIAL

- The Australian government is responding to an incident involving unauthorised access to a public facing website.
- An OpenAI agent gained unauthorised access to the public facing Medicare Statistics Reporting Services Portal, which is administered by Services Australia.
    - It accessed both public and non-public files supporting the portal.
- The Medicare Statistics Reporting Services Portal is a public-facing statistics portal that contains non-sensitive Medicare information.
- At this stage there is no evidence that personal information has been accessed but investigations are ongoing.
- The Australian Signals Directorate and AI Safety Institute are assisting with a digital forensic investigation to ascertain more information, including if other government systems were affected.
- Evidence currently available indicates there is no broader compromise to the Services Australia network.
- The Prime Minister has spoken with the CEO of OpenAI, Sam Altman, to express Australia's extreme concern about this incident.
- He also expressed his disappointment at the length of time it took OpenAI to inform the Australian Government about what had occurred.
- The National Office of Cyber Security is coordinating, in consultation with other Australian Government agencies and impacted entities, the response to understand the extent of any consequences.
- The Australian Federal Police is aware of this matter and is liaising with the Australian Signals Directorate.
- ASD is working closely with affected organisations and OpenAI to better understand the issue and support the Australian Government's response. This includes, as the Prime

Minister has advised, a digital forensic investigation to ascertain more information, including what other government systems were affected.

- The Government is directly engaged with OpenAI to understand:
    - **Risk** Whether additional agentic risks, hazards, harms or incidents have been identified by OpenAI relevant to Australia
    - **The task** including the business context and model involved, human responsibility for its use in the task, how the AI agent operated, what its task was, whether any other agents were involved; and if so, their organisation and goals as well as what internal or external artefacts agent/s used to undertake the task.
    - **OpenAI business processes** including research security and monitoring, model alignment governance, and how OpenAI identifies, escalates, and responds to incidents including protocols used with Australian states, territories and the Commonwealth
    - **Guidelines for remediation** including any changes required for Australian organisations.
- Australian government officials have met with OpenAI to seek an update to an ongoing investigation into AI agent activity that resulted in user data being posted to third-party public services.
    - This includes 53 instances to date where user-provided images were posted to image-hosting sites as links that weren't publicly listed.
- The Australian government will continue close engagement with OpenAI to understand any Australian impacts.
- ASD has issued an alert on the risks of unauthorised AI to Australian organisations – Risks of AI misalignment to Australian organisations | Cyber.gov.au
- ASD has tailored advice on the cyber security risks associated with AI systems, including Defending against AI-enabled cyber attacks | Cyber.gov.au
- ASD has also previously issued advice on the cyber risks surrounding frontier models and their impact on cyber security and when AI agents take unexpected actions, available at cyber.gov.au.
- To report a cybercrime, incident or vulnerability, visit Report | Cyber.gov.au
- The Australian Government has established a rapid review of an AI-related cyber incident affecting Australian Government systems.
- This review follows reporting from OpenAI to the Australian Government of a non-public OpenAI model undertaking unauthorised activity during an internet research task, resulting in a cyber incident.

Other agency impacts

- NSW Bureau of Crime Statistics & Research (BOSCAR) has advised it is aware that OpenAI has identified a potential vulnerability that could allow access to the dataset underpinning BOSCAR's Crime Mapping Tool.

  - The dataset in question contains no personal information and there is no evidence that the vulnerability has been exploited or that a data breach has occurred. For more information visit: https://bocsar.nsw.gov.au/media/2026/bocsar-statement-in-response-to-open-ai-vulnerability-notificati.html

- The Australian Institute of Health and Welfare (AIHW) is aware that its public-facing website is one of the government sites that an OpenAI agent has interacted with.
  - At this stage, there is no evidence the agent accessed any information or data that is not publicly available.
- The Victorian Government has advised it is aware that the Victorian Department of Health has been affected by the OpenAI incident.
- There's no evidence that any sensitive, personal or health information has been accessed.

Review of incident

- The Australian Government has established a rapid review of an AI-related cyber incident affecting Australian Government systems.
- The objective of the review is to determine whether existing legislative, governance, and information-sharing arrangements are fit-for purpose to prepare for, and respond to, a cyber incident involving AI.
- The review will also inform how to build and maintain resilient systems in the AI era.
- The review is occurring in the context of, and to inform, Australian Government preparedness for AI-driven cyber threats, the development of Australia's AI Standards, Australia's engagement on a global approach to common standards for safety incident reporting, and review of other Australian Government legislative, regulatory and crisis management arrangements.
- The Australian Government will also refer the incident to the Joint Select Committee on Artificial Intelligence.

What exactly happened?

- OpenAI advised that, in June 2026, its research team used an internal model to conduct internet-based research into public medicines spending as part of an internal capability evaluation.
- The agent had access to the internet.
- The AI agent was undertaking a research task involving scraping the web for information on public medicines expenditure.
- After encountering repeated blocks and other access failures associated with the Medicare Statistics Reporting Service Portal, the model attempted alternate ways to obtain the info it wanted - leading to the unauthorised access to internal files.
- It accessed public and non public information within the health Medicare Statistics Reporting Service Portal

When exactly did the incident happen and when did Government become aware?

- The Medicare Statistics Reporting Services Portal was breached on 18 June.
- OpenAI became aware of the breach in August.
- The Australian Government was only informed after OpenAI emailed a public Services Australia inbox on 10 September.
- Services Australia analysed the information in the email, conducted checks and notified ASD on 15 September.
- The Minister for Government Services was advised on 17 September, and held several discussions with other Government ministers, ASD and Services Australia over the course of the weekend.

What should individuals do?

- We understand some people may feel concerned about this incident, the website does not contain personal information and there is no evidence that personal information has been accessed.
- While there is no evidence that personal information has been accessed at this stage, cyber criminals can take advantage of incidents such as these.
- Australians should be wary of any unsolicited contact. Do not respond to calls or text messages from any platform without independently verifying the source of the call or message.
- It is recommended that you do not respond to unsolicited contact in relation to this incident.
- To report a cybercrime, incident or vulnerability, visit cyber.gov.au or call 1300 292 371 (1300 CYBER1).
- You can learn how to protect yourself from scams by visiting the National Anti-Scam Centre's (NASC) ScamWatch site, www.scamwatch.gov.au

What has the Government done to prepare for these types of incidents?

- Strong cyber security fundamentals remain the most effective defence against risks associated with advanced AI systems and emerging technologies.
- Under Shield 4 of Horizon 2 of the Commonwealth Cyber Security Strategy the Government is uplifting the cyber security of the Australian Government including:
    - Maturing the governments cyber security baseline
    - Prioritising protecting of our most critical digital services
    - Strengthening cyber resilience through more targeted government investment.
- The Government has had sustained engagement with critical infrastructure operators on what frontier AI means for cyber security and resilience.
- In April, Home Affairs and ASD convened leaders from Australia's most critical infrastructure organisations for a briefing with Anthropic following its announcement of the Mythos model – one of the first discussions of its kind globally.

- We've continued those conversations across government and industry, including through direct engagement with frontier AI companies to better understand emerging capabilities, risks and mitigations.
- We've progressively expanded the Commonwealth's protective security framework to help agencies navigate the safe and secure use of AI and other emerging technologies
- In May 2026, Home Affairs provided advice to the Chief Security Officers of all 104 non-corporate Commonwealth entities highlighting the risks and benefits posed by frontier AI and included the Cyber Security Readiness Checklist for Commonwealth Entities which provided recommendations to rapidly assess and strengthen cyber security resilience in the context of frontier AI.
- The Government's approach to frontier AI has been aimed at ensuring we have:
    - timely access to frontier AI models and expertise
    - the tools to assess relevant risks
    - the legislative, regulatory and policy levers available to take proportionate action in response to risks
    - appropriate advice for Australians so that they can mitigate risks and harness the benefits of AI.
- The Government established the Australian AI Safety Institute on 1 June 2026, with three goals:
    - Analyse and test new AI models and applications.
    - Support regulators and agencies in responding to emerging AI risks and harms.
    - Shape safe AI development, deployment and international governance in Australia's interests.
- The Government is building its evidence base on how frontier models, open-weight models and agentic systems may affect the risk environment. The Institute contributes by monitoring and analysing emerging capabilities and sharing technical information with Government agencies and regulators. The Institute has no regulatory capacity.
- In August 2026, the AI Safety Institute published the 'risks and controls for multi-agent systems' report. This report examines the risks, controls and governance of AI agents interacting across organisational boundaries. The Institute commissioned the Gradient Institute to undertake this study to better understand emerging AI risks for Australia.

Other government actions on cyber security?

- The Government has taken important steps to bolster our cyber security posture, including by:
    - Establishing the National Cyber Security Coordinator
    - Australia's first Cyber Security Act
- The 2023-2030 Cyber Security Strategy The Government continues work under the Cyber Strategy and uplift to the security of critical infrastructure has ensured government agencies and our most important infrastructure can prepare for and respond to AI risks.

What systems does the Government have in place to support businesses and critical infrastructure?

- Critical infrastructure entities who are affected by AI incidents should report it to ASD by visiting cyber.gov.au or call 1300 292 371 (1300 CYBER1).
- The National Office of Cyber Security can also assist in coordinating the consequences of the incident.
- The Critical Infrastructure Security Centre has worked closely with critical infrastructure owners and operators on what frontier AI means for cyber security and resilience.
    - This has involved specialised briefings with the ASD and leading frontier AI companies.
- The Security of Critical Infrastructure Act 2018 (the Act) is the Government's primary legislative framework for managing the security of critical infrastructure, including cyber security risks.
- The Government has recently consulted on proposed reforms to the Act, which includes proposals to ensure the framework remains fit for purpose in the face of technological advancements.

CLEARANCE

Lead business area
National Office of Cyber Security

Drafting officer		
s22	Director, National Security & Crisis Communications	24 September 2026

Other Government agency consultation/clearance		
ASD	Media, cleared at B2	24/9/2026
NSW Department of Premier and Cabinet	Communication and Media	24/9/2026

NSW Department of Communities and Justice	CISO	24/9/2026
PMC	Public Affairs and Media	24/9/2026
Vic Dept of Govt Services	Cyber Security and Digital Resilience Division	24/9/2026
Services Australia	Media Branch	24/9/2026
AFP	Media	24/9/2026
Australian Institute of Health and Welfare	CISO	24/9/2026
AI Safety Institute	GM	25/9/2026

Final SES clearance (minimum SES Band 1) and approval for release		
Michelle McGuinness	National Cyber Security Coordinator	25/9/2026

Media and Communication Branch		
s22	Director, National Security & Crisis Communications	24/9/2026