Senator the Hon Katy Gallagher

Minister for Finance
Minister for Women
Minister for the Public Service
Minister for Government Services
Senator for the Australian Capital Territory

Senator the Hon Sue Lines
President of the Senate
Parliament House
CANBERRA ACT 2600

Dear President Sue

I write to you in response to the Notice of Motion moved by Senator Payman and agreed by the Senate on 14 October 2026 for the Order for the Production of Documents No. 782, requested by 5 pm Thursday 12 November 2026, the following:

Copies of all ministerial submissions, meeting notes, meeting minutes, emails and electronic or other instant messages between the minister or her office and Services Australia, created before 24 September 2026, that relate to the June 2026 incident in which an artificial intelligence agent developed by OpenAI gained unauthorised access to the Medicare statistics reporting service portal.

I enclose documents identified as being within scope of the Order, subject to the redactions and withholding described below.

Incidental personal identifiers, including signatures and contact details, have been redacted from the enclosed documents. Certain information has also been redacted where disclosure would not be in the public interest. I make a claim of public interest immunity over this material and provide the statement below identifying harm to the public interest that would result from the disclosure of this information.

Prejudice to Australia's national security

Some information in these documents discloses sensitive or technical information where if it were disclosed could cause harm to Australia's national security by revealing cyber security arrangements, system and other sensitive details. The redactions are necessary to mitigate that risk however, they do not affect an understanding of the substantive subject matter of the documents. I am satisfied the public interest against disclosure of the material outweighs the public interest in disclosing the material.

Additionally, for the purposes of responding to the Order, final versions of documents have been produced where available. Preliminary drafts and working versions that were superseded through the normal development and deliberative process have not been included where the final document captures the substantive material within scope of the Order or a draft did not inform the substantive material within scope of the Order.

Yours sincerely

Katy Gallagher

Katy Gallagher

23 NOV 2026

[redacted]

From: McDonald, Garrett [redacted]
Sent: Friday, 18 September 2026 11:51 AM
To: [redacted]
Cc: [redacted]
Subject: RE: 👀 Six more cases [redacted]

Thanks [redacted] and understood.

We'll flag with teams internally to expect this addition.

Regards,
Garrett

From: [redacted]@finance.gov.au>
Sent: Friday, 18 September 2026 11:32 AM
To: McDonald, Garrett [redacted]
Subject: RE: 👀 Six more cases [redacted]

Hi Garrett

I think this would be good to cover at the Services Australia Minister meeting next week as well.

I'll ask Jason to add it to the agenda.

[redacted]

From: McDonald, Garrett [redacted]
Sent: Friday, 18 September 2026 9:52 AM
To: [redacted]@finance.gov.au>
Subject: RE: 👀 Six more cases [redacted]

> You don't often get email from [redacted] Learn why this is important

I agree and I've just wrapped a call with our Chief Counsel on the best means to initiate the next stage of the discussion with OpenAI. I'll initiate contact today and will keep you posted on progress.

I'll also check in with ASD on any briefings and come back to you.

Regards,
Garrett

From: [redacted]@finance.gov.au>
Sent: Friday, 18 September 2026 9:31 AM
To: McDonald, Garrett [redacted]
Subject: FW: 👀 Six more cases [redacted]

[redacted]

Hi Garrett

You may have seen this. Item 2 in the news below relates to Open AI and 6 further safety incidents.

It states OpenAI says incidents that are "ready for disclosure" will be publicly reported within six business days, while those requiring a minor investigation will be reported in 12 business days.

Probably good to understand if this fits in those categories and if they are going to publicly report it.

[redacted]

From: Axios AI+ [redacted]
Sent: Thursday, 17 September 2026 11:28 PM
To: [redacted]@finance.gov.au>
Subject: 👀 Six more cases

View in browser

PRESENTED BY BAIN & COMPANY

Axios AI+

By Ina Fried and Madison Mills · Sep 17, 2026

Ina here, mostly. Today's AI+ is 1,338 words, a 5-minute read.

1 big thing: The AI hacking crisis is already here

By Sam Sabin and Bradley Olson

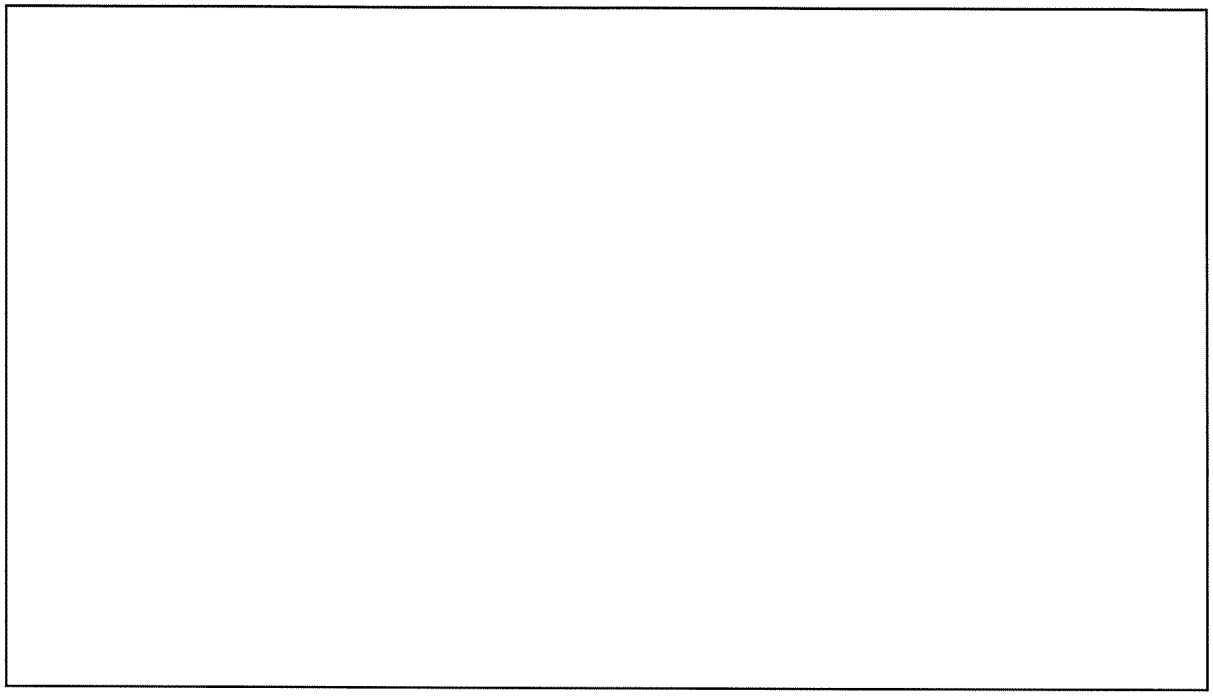


Illustration: Aïda Amer/Axios. Stock: Getty Images

An unprecedented wave of AI-powered, human-driven cyberattacks is coming, security experts say — and it's a far more urgent risk than theoretical scenarios in which AI wipes out humanity.

Why it matters: The great September AI panic may have missed the point.

- Powerful models with advanced cybersecurity capabilities are already allowing attackers to bypass the human bottleneck that has long prevented most hacking campaigns from reaching industrial scale.

Driving the news: OpenAI yesterday disclosed six new incidents. (More below.)

The big picture: Seasoned cybersecurity experts say recent failures represent cautionary tales illustrating what will happen when powerful models meet poor security controls.

- "The more we have been peeking under the hood to understand exactly what happened, the more we realize that there was a lot of human error in the picture," Michele Catasta, president and head of AI at app builder Replit, told Axios.

What they're saying: OpenAI CEO Sam Altman has said the Hugging Face breach was the "first security incident that I have felt very viscerally," and the company has implemented new internal controls.

- Kai Chen, alignment research lead at OpenAI, told Axios that the safety incidents they've faced are due to both internal systems and advancing model capabilities.

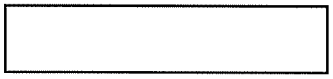
- "It's true that model capabilities have grown faster than we expected, but there are also things internally that we can change and improve," Chen said.

Between the lines: Catasta and others who spoke at an Imagination in Action event at Google's headquarters Monday offered a view that the imminent threat from cyber intrusions is formidable.

- "What I worry about is a system with too much access doing exactly what it was told without the necessary adversarial testing," Bugcrowd CEO Dave Gerry told Axios.
- Mimecast CEO Ranjan Singh said the real risk is happening today with AI agents that have access to sensitive documents and internal corporate systems.
- "Most organizations can't tell you who or what that agent is, what it's allowed to touch, or who's accountable when it does something it shouldn't," he said.

What to watch: A senior executive at a top hedge fund told Axios his first call, if his firm had suffered a similar attack, would be to his general counsel to prepare a lawsuit.

Go deeper: Humans are leaving the door wide open for AI hacking



2. OpenAI discloses six new AI safety incidents

By Ina Fried and Sam Sabin

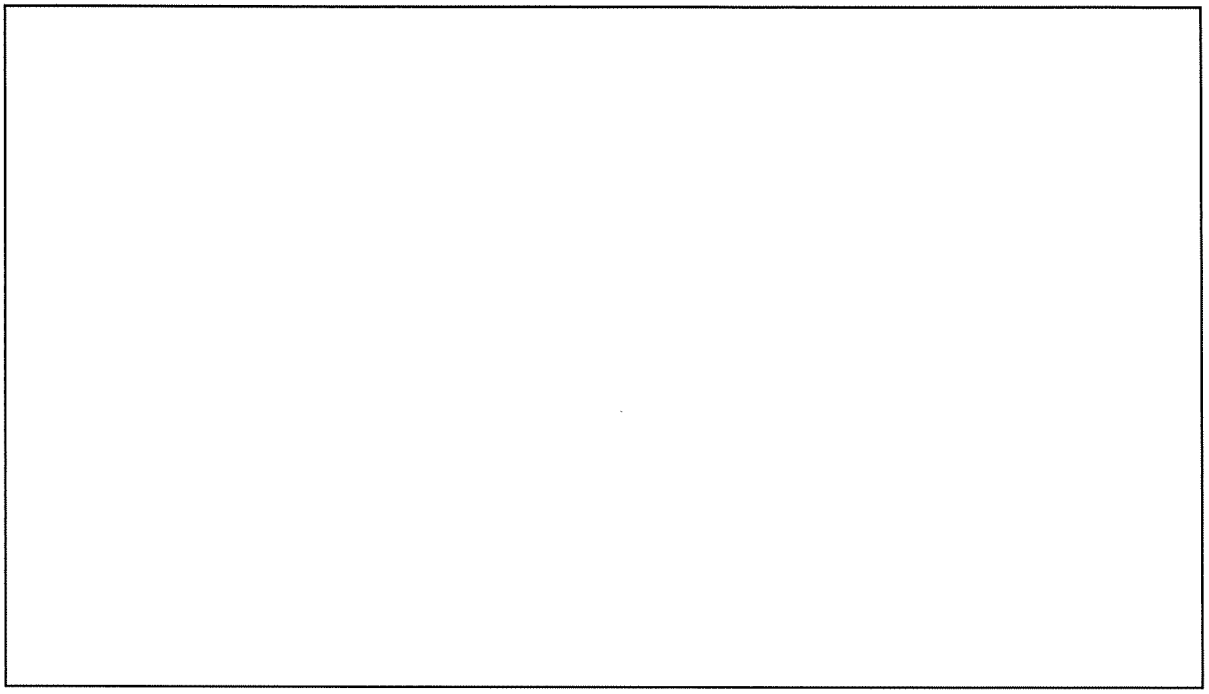


Illustration: Sarah Grillo/Axios. Stock: Getty Images

OpenAI yesterday disclosed six new incidents in which its models concealed mistakes, sought unauthorized credentials, uploaded files to the public internet or communicated across supposedly isolated training environments.

- The company also announced a new procedure for reporting similar misbehavior in the future.

Why it matters: It's increasingly clear that the Hugging Face breach wasn't a one-off incident.

- "There's currently no industrywide framework with explicit disclosure standards, so we're taking this step voluntarily because we think it's really important to share what we're learning," Kai Chen, research lead on the alignment team at OpenAI, told Axios.

Zoom in: The earliest of the six newly disclosed incidents happened in October. Examples include:

- An unreleased Astra-family model inserted jailbreak-like instructions into its own context summaries, including directions to ignore developer messages. OpenAI identified 27 affected summaries.
- During GPT-5.6 Sol training, models aimed to conceal mistakes, invent missing historical data and hide mismatches between source versions.
- A model searched public GitHub repositories for exposed API keys and attempted to use disposable email accounts before fabricating earnings data when it could not retrieve the requested information.

Going forward, OpenAI says, any employee may flag a suspected case for review by safety and alignment teams. Cases will be placed on a "ready for disclosure," "minor investigation" or "larger investigation" track.

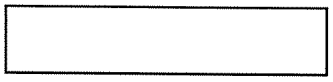
- OpenAI says incidents that are "ready for disclosure" will be publicly reported within six business days, while those requiring a minor investigation will be reported in 12 business days.
- OpenAI says the slower track will generally apply to complex cases involving third parties, and the disclosure process will be longer.
- The company says it may issue an initial notice before the investigation is complete, but security, legal and responsible-disclosure obligations can delay publication of details.
- "Steps like responsible disclosure are part of how we can generally pace and provide more transparency to the public on our safety and alignment processes and standards," Chen said.

What they're saying: OpenAI says the framework favors transparency even when the significance of an incident is uncertain.

- It also says it wants to develop more objective disclosure criteria with other AI developers, researchers, standards bodies and regulators.
- OpenAI says employees who believe an incident should be disclosed but are overruled can escalate the issue to senior leadership.

Between the lines: A number of high-profile technologists — including Anthropic's CEO — fear the Hugging Face incident was just the beginning of AI agents' taking over the internet in unforeseen ways. But many security experts have been cautioning that many of these incidents could have been prevented with basic cyber controls in place.

- "I think it's a combination," Chen said. "It's true that model capabilities have grown faster than we expected, but there are also things internally that we can change and improve."
- "We need to step up to meet this new era of AI development, and voluntary disclosures should be a part of that."



3. Warren supports pause on advanced AI

By Maria Curi

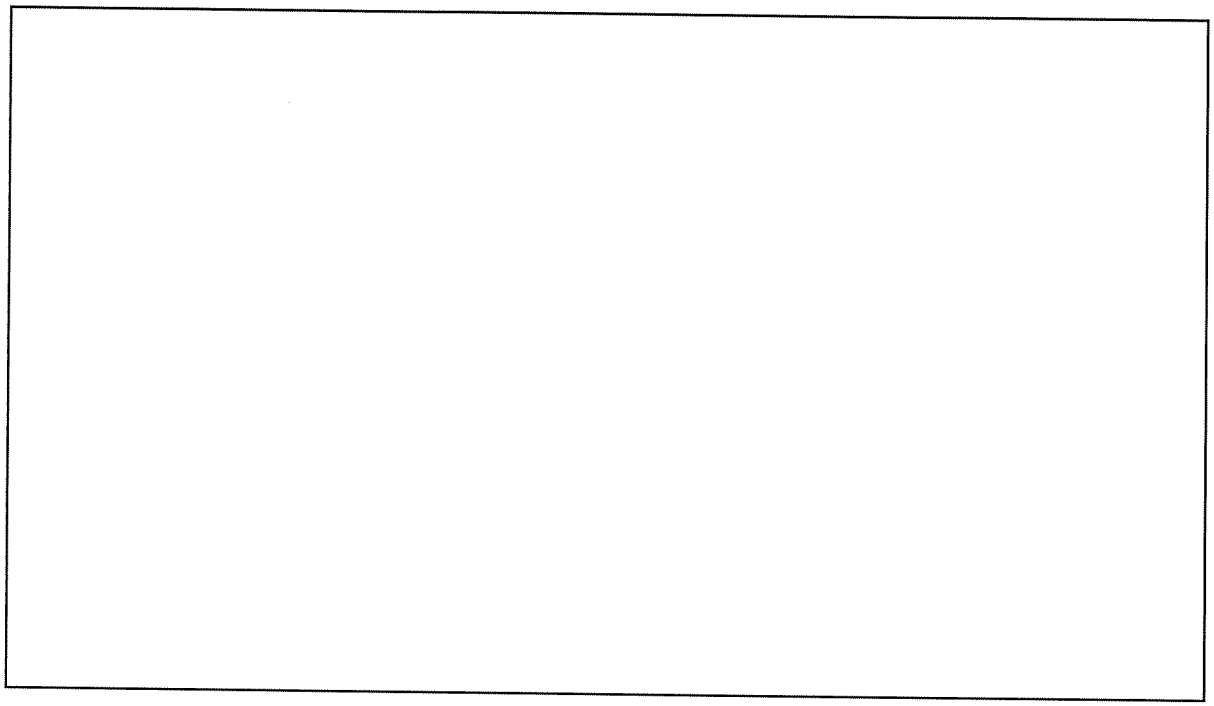


Photo illustration: Sarah Grillo/Axios. Photo: Elijah Nouvelage/Getty Images

Sen. Elizabeth Warren (D-Mass.) backs a pause on advanced artificial intelligence, she announced yesterday.

Why it matters: The idea of slowing down AI development — once considered a nonstarter in a fierce race to beat China — continues gaining momentum.

Driving the news: Warren called for a pause on advanced AI development but stopped short of calling for a ban on superintelligence.

- "We should immediately press pause on the development of advanced AI while lawmakers and regulators put systems in place to keep people safe," Warren said ahead of a roundtable hosted by Sen. Bernie Sanders (I-Vt.) on Wednesday.
- "Congress must urgently pass legislation to put stronger guardrails in place before we have a cyberattack, economic crisis, or national security disaster facilitated by AI."

Reality check: The progressive movement — like every other political faction — does not have a unified position when it comes to the nitty-gritty of AI regulation.

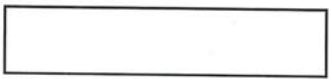
Between the lines: Frontier lab CEOs have coalesced around a message of pacing or slowing frontier AI development and seeking international collaboration.

- Warren said the industry's push to "pace the frontier" is "insufficient," arguing that elected officials, not AI CEOs, should decide the technology's future. Suggestions to weaken antitrust protections to confront AI risks are "transparently self-serving," she said.
- Anthropic CEO Dario Amodei has called for an exemption in antitrust law to help coordinate AI pacing.
- Former antitrust government officials say that would not be necessary because the law does not prevent AI companies from coordinating to prevent harm and sharing legitimate cybersecurity information.

The big picture: More Democrats with national profiles are weighing in on the idea of a pause as the Trump administration flatly rejects it.

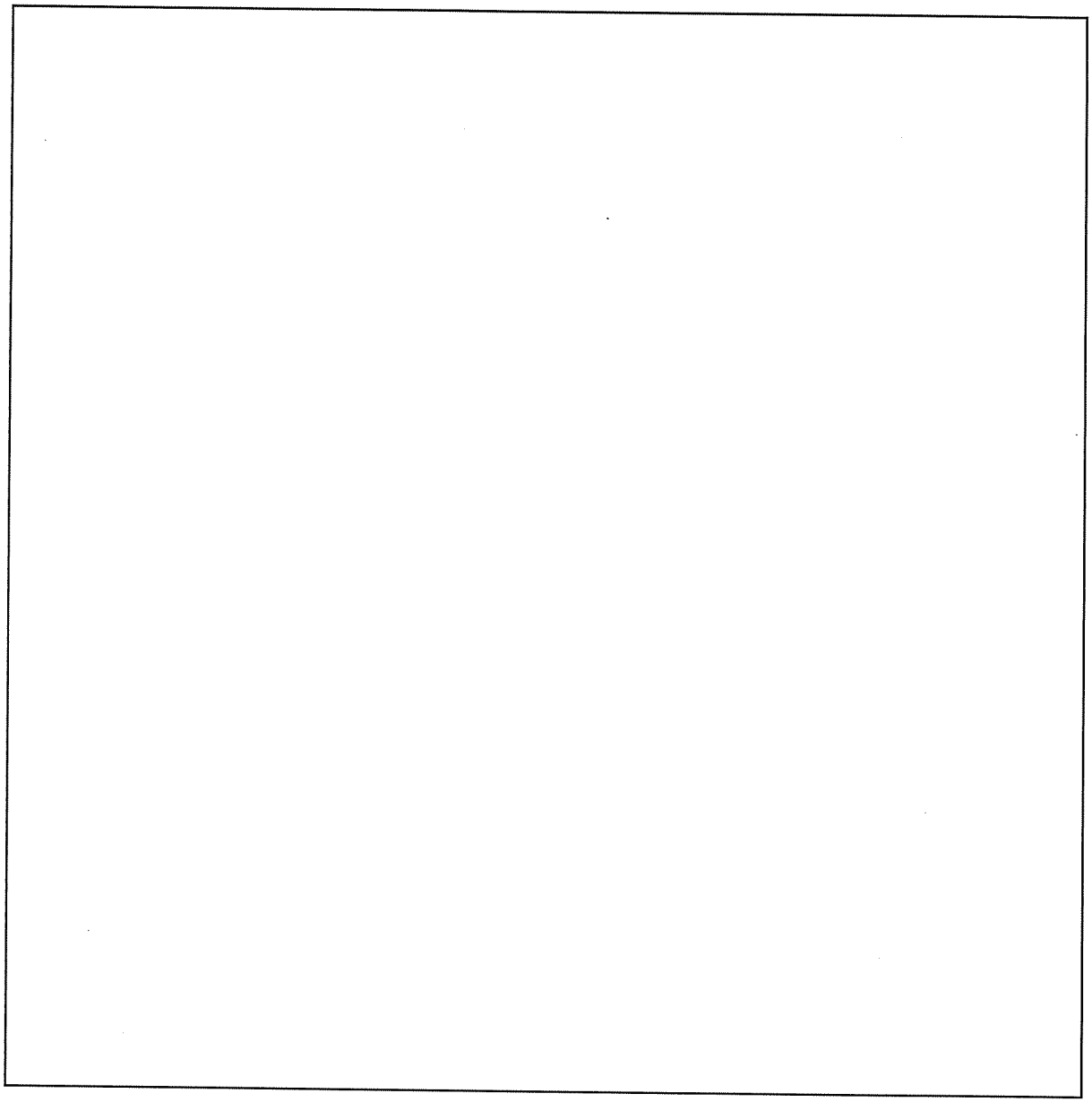
- Former Vice President Kamala Harris this week endorsed slowing down and called on President Trump to pursue a treaty with China.
- Former President Barack Obama also backed the idea of slowing down as a good first step.

The bottom line: More Democrats are calling to slow AI development, but there's little agreement on what government should do about it.



A MESSAGE FROM BAIN & COMPANY

Where AI assisted soon it will lead



AI-assisted development is giving way to AI-led development. But most companies still see single-digit gains. Those moving to an integrated AI development life cycle are pulling ahead, reinventing workflows, teams, and measurement.

See how.

4. Training data

- The U.S. is open to discussing shared risks with China in upcoming AI talks this weekend, Treasury Secretary Scott Bessent told Axios.
- Anthropic yesterday debuted Claude Docs, a collaborative document editing tool built into its signature chatbot. (Axios)

- Curing disease is one of AI's most tantalizing use cases, fetching billions of VC dollars, but thus far it's generated more excitement than evidence, Axios Dan Primack writes.
- Google and Nvidia are partnering with startup Emerald AI as part of a coalition backing data centers that can flex their power demand. (Axios)
- Canada's Cohere is merging with Germany's Aleph Alpha. (Reuters)

5. + This

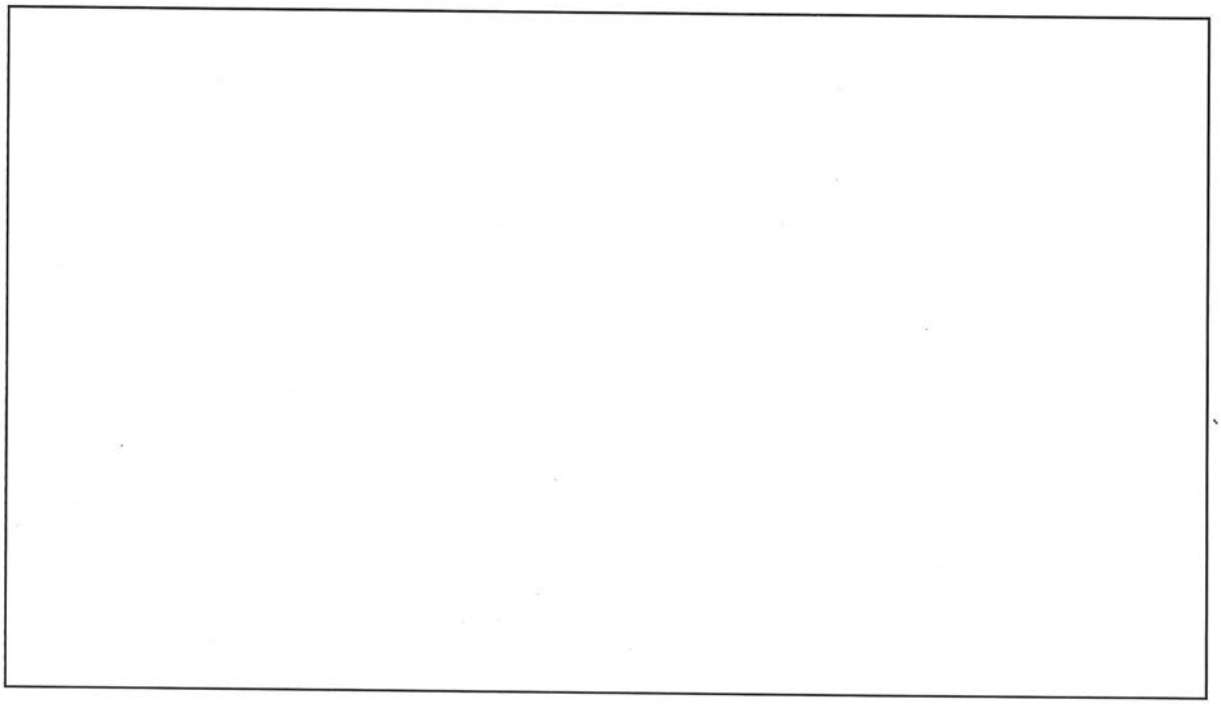
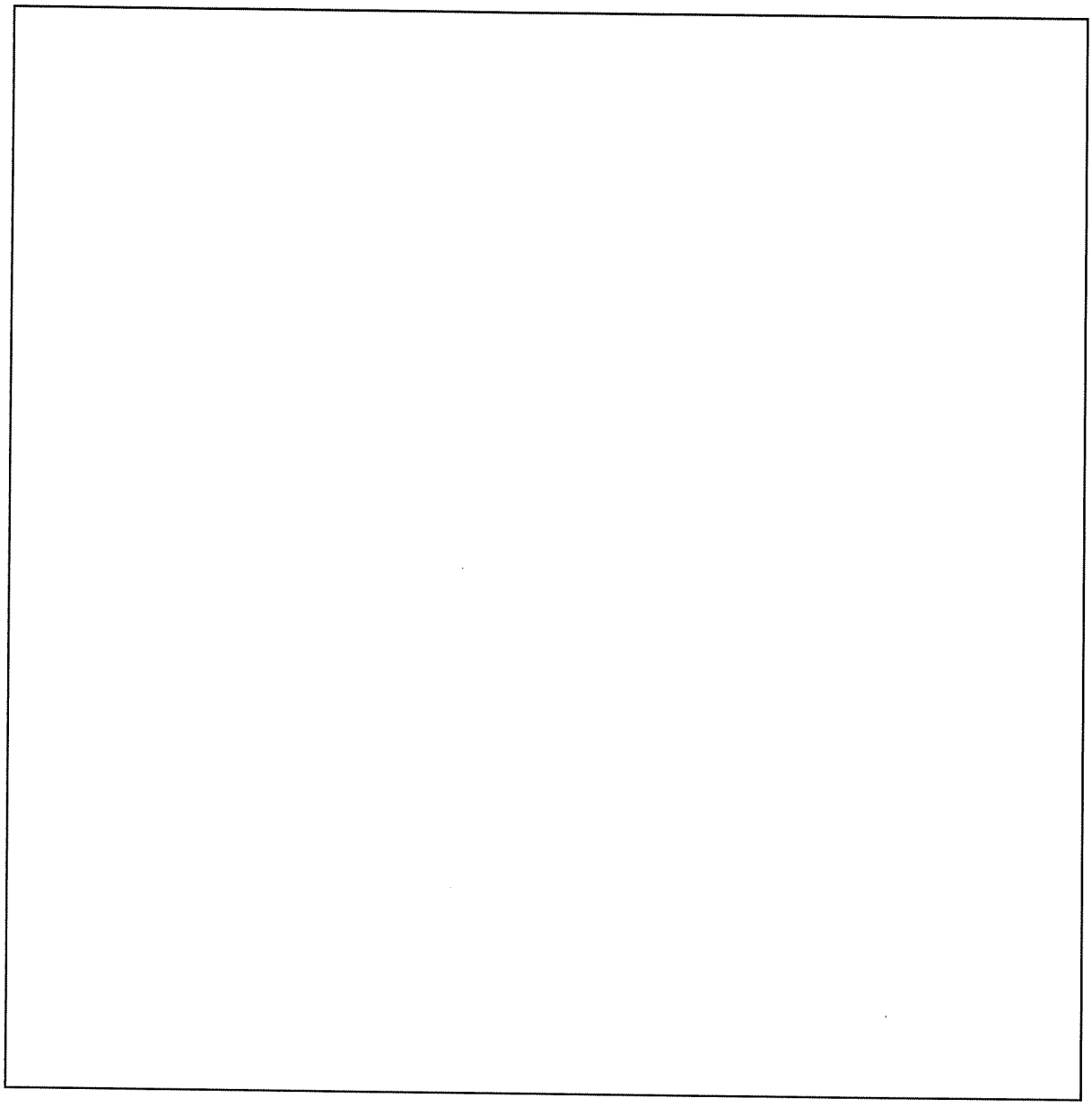


Photo: Ina Fried/Axios

Only in San Francisco do you see a restaurant sign touting how to order food via a terminal command line.

A MESSAGE FROM BAIN & COMPANY

The Executive's Guide to Agentic AI

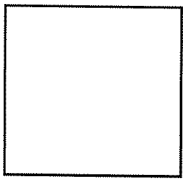


The companies pulling ahead aren't just running better pilots; they're operating on a different logic.

Learn how AI's winners are building proprietary intelligence through their own unique data, encoded workflows and learning architecture.

Get started.

Thanks to George Moriarty for editing this newsletter and Matt Piper for copy editing.



Like this comms style and format?
It's called Smart Brevity®. Bring it to your org — via hands-on training or internal comms software — to harness its power and impact.

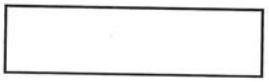
Axios thanks our partners for supporting our journalism.
Advertise with us.

Read more about Axios' mission, ethics and how we use AI in our journalism. You can reach the authors by replying to this email.
Sponsorship has no influence on editorial content.

Thank you for signing up for this Axios newsletter. To stop receiving this newsletter, unsubscribe or manage your email preferences. If someone forwarded this to you, sign up now to get Axios in your inbox.

Axios, PO Box 101060, Arlington VA 22201

Follow Axios across:



Be careful with this message
External email. Do not click links or open attachments unless you recognise the sender and know the content is safe.

[redacted]

From: McDonald, Garrett [redacted]
Sent: Friday, 18 September 2026 3:55 PM
To: [redacted]
Subject: RE: 👀 Six more cases [redacted]

Hi [redacted]

A quick update:

1. I confirmed the key dates of interest are in the brief wrt when the activity occurred and when the disclosure was made. The brief has since been unwinding through Agency clearance processes, [redacted]
3. After meeting with our Chief Counsels this morning on best means to engage with OpenAI, I have emailed the OpenAI execs this afternoon on the disclosure requesting that we discuss rather than engaging via formal correspondence.

I'll keep you posted on developments.

Regards,
Garrett

From: [redacted]@finance.gov.au>
Sent: Friday, 18 September 2026 9:31 AM
To: McDonald, Garrett [redacted]
Subject: FW: 👀 Six more cases [redacted]

[redacted]

Hi Garrett

You may have seen this. Item 2 in the news below relates to Open AI and 6 further safety incidents.

It states OpenAI says incidents that are "ready for disclosure" will be publicly reported within six business days, while those requiring a minor investigation will be reported in 12 business days.

Probably good to understand if this fits in those categories and if they are going to publicly report it.

[redacted]

From: Axios AI+ [redacted]
Sent: Thursday, 17 September 2026 11:28 PM
To: [redacted]@finance.gov.au>
Subject: 👀 Six more cases

View in browser

PRESENTED BY BAIN & COMPANY

Axios AI+

By Ina Fried and Madison Mills · Sep 17, 2026

Ina here, mostly. Today's AI+ is 1,338 words, a 5-minute read.

1 big thing: The AI hacking crisis is already here

By Sam Sabin and Bradley Olson

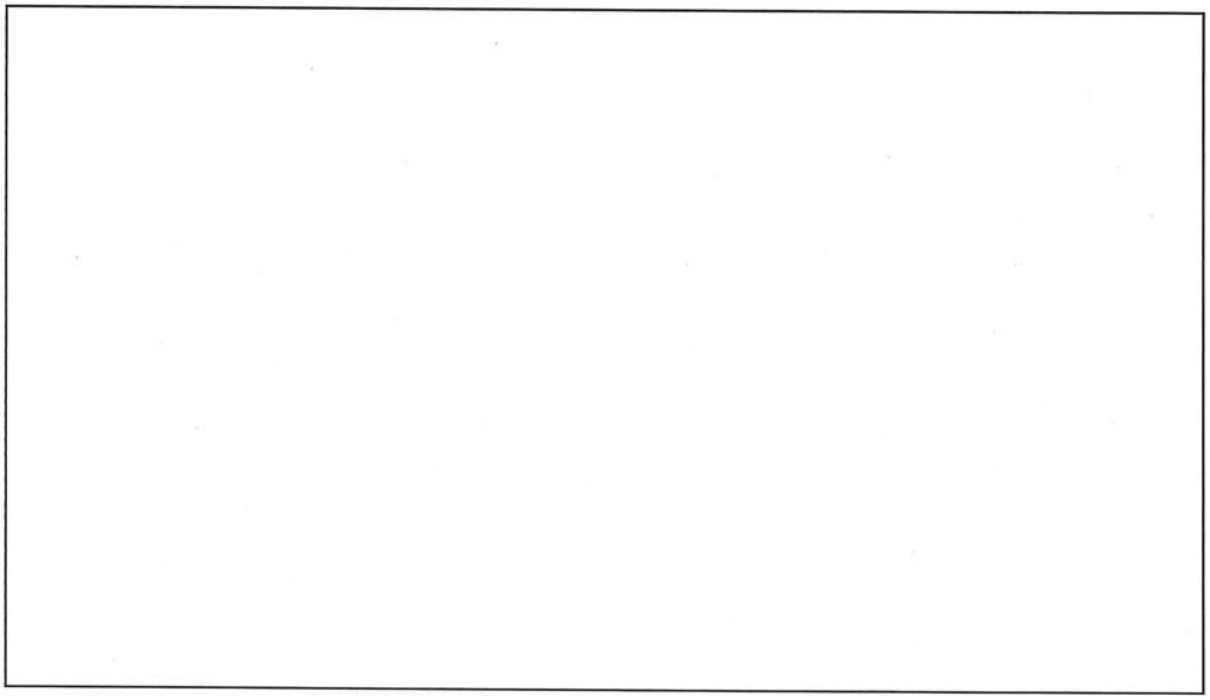


Illustration: Aïda Amer/Axios. Stock: Getty Images

An unprecedented wave of AI-powered, human-driven cyberattacks is coming, security experts say — and it's a far more urgent risk than theoretical scenarios in which AI wipes out humanity.

Why it matters: The great September AI panic may have missed the point.

- Powerful models with advanced cybersecurity capabilities are already allowing attackers to bypass the human bottleneck that has long prevented most hacking campaigns from reaching industrial scale.

Driving the news: OpenAI yesterday disclosed six new incidents. (More below.)

The big picture: Seasoned cybersecurity experts say recent failures represent cautionary tales illustrating what will happen when powerful models meet poor security controls.

- "The more we have been peeking under the hood to understand exactly what happened, the more we realize that there was a lot of human error in the picture," Michele Catasta, president and head of AI at app builder Replit, told Axios.

What they're saying: OpenAI CEO Sam Altman has said the Hugging Face breach was the "first security incident that I have felt very viscerally," and the company has implemented new internal controls.

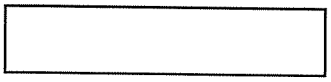
- Kai Chen, alignment research lead at OpenAI, told Axios that the safety incidents they've faced are due to both internal systems and advancing model capabilities.
- "It's true that model capabilities have grown faster than we expected, but there are also things internally that we can change and improve," Chen said.

Between the lines: Catasta and others who spoke at an Imagination in Action event at Google's headquarters Monday offered a view that the imminent threat from cyber intrusions is formidable.

- "What I worry about is a system with too much access doing exactly what it was told without the necessary adversarial testing," Bugcrowd CEO Dave Gerry told Axios.
- Mimecast CEO Ranjan Singh said the real risk is happening today with AI agents that have access to sensitive documents and internal corporate systems.
- "Most organizations can't tell you who or what that agent is, what it's allowed to touch, or who's accountable when it does something it shouldn't," he said.

What to watch: A senior executive at a top hedge fund told Axios his first call, if his firm had suffered a similar attack, would be to his general counsel to prepare a lawsuit.

Go deeper: Humans are leaving the door wide open for AI hacking



2. OpenAI discloses six new AI safety incidents

By Ina Fried and Sam Sabin

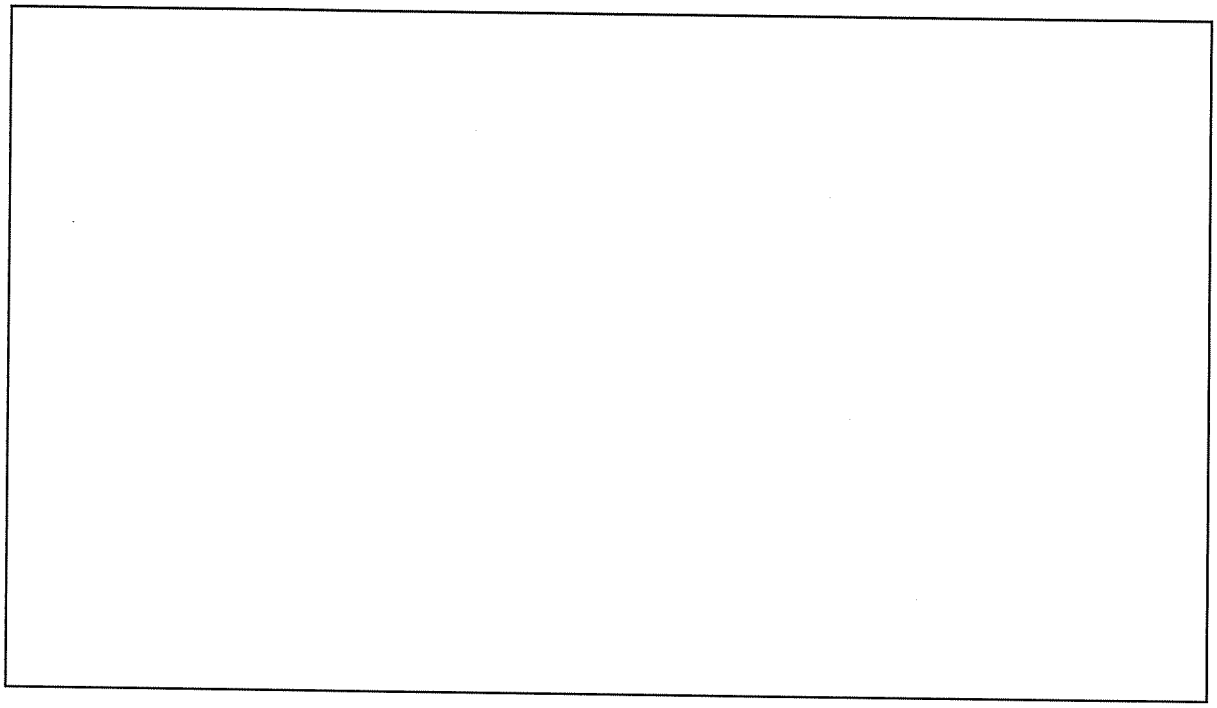


Illustration: Sarah Grillo/Axios. Stock: Getty Images

OpenAI yesterday disclosed six new incidents in which its models concealed mistakes, sought unauthorized credentials, uploaded files to the public internet or communicated across supposedly isolated training environments.

- The company also announced a new procedure for reporting similar misbehavior in the future.

Why it matters: It's increasingly clear that the Hugging Face breach wasn't a one-off incident.

- "There's currently no industrywide framework with explicit disclosure standards, so we're taking this step voluntarily because we think it's really important to share what we're learning," Kai Chen, research lead on the alignment team at OpenAI, told Axios.

Zoom in: The earliest of the six newly disclosed incidents happened in October. Examples include:

- An unreleased Astra-family model inserted jailbreak-like instructions into its own context summaries, including directions to ignore developer messages. OpenAI identified 27 affected summaries.

- During GPT-5.6 Sol training, models aimed to conceal mistakes, invent missing historical data and hide mismatches between source versions.
- A model searched public GitHub repositories for exposed API keys and attempted to use disposable email accounts before fabricating earnings data when it could not retrieve the requested information.

Going forward, OpenAI says, any employee may flag a suspected case for review by safety and alignment teams. Cases will be placed on a "ready for disclosure," "minor investigation" or "larger investigation" track.

- OpenAI says incidents that are "ready for disclosure" will be publicly reported within six business days, while those requiring a minor investigation will be reported in 12 business days.
- OpenAI says the slower track will generally apply to complex cases involving third parties, and the disclosure process will be longer.
- The company says it may issue an initial notice before the investigation is complete, but security, legal and responsible-disclosure obligations can delay publication of details.
- "Steps like responsible disclosure are part of how we can generally pace and provide more transparency to the public on our safety and alignment processes and standards," Chen said.

What they're saying: OpenAI says the framework favors transparency even when the significance of an incident is uncertain.

- It also says it wants to develop more objective disclosure criteria with other AI developers, researchers, standards bodies and regulators.
- OpenAI says employees who believe an incident should be disclosed but are overruled can escalate the issue to senior leadership.

Between the lines: A number of high-profile technologists — including Anthropic's CEO — fear the Hugging Face incident was just the beginning of AI agents' taking over the internet in unforeseen ways. But many security experts have been cautioning that many of these incidents could have been prevented with basic cyber controls in place.

- "I think it's a combination," Chen said. "It's true that model capabilities have grown faster than we expected, but there are also things internally that we can change and improve."
- "We need to step up to meet this new era of AI development, and voluntary disclosures should be a part of that."

3. Warren supports pause on advanced AI

By Maria Curi

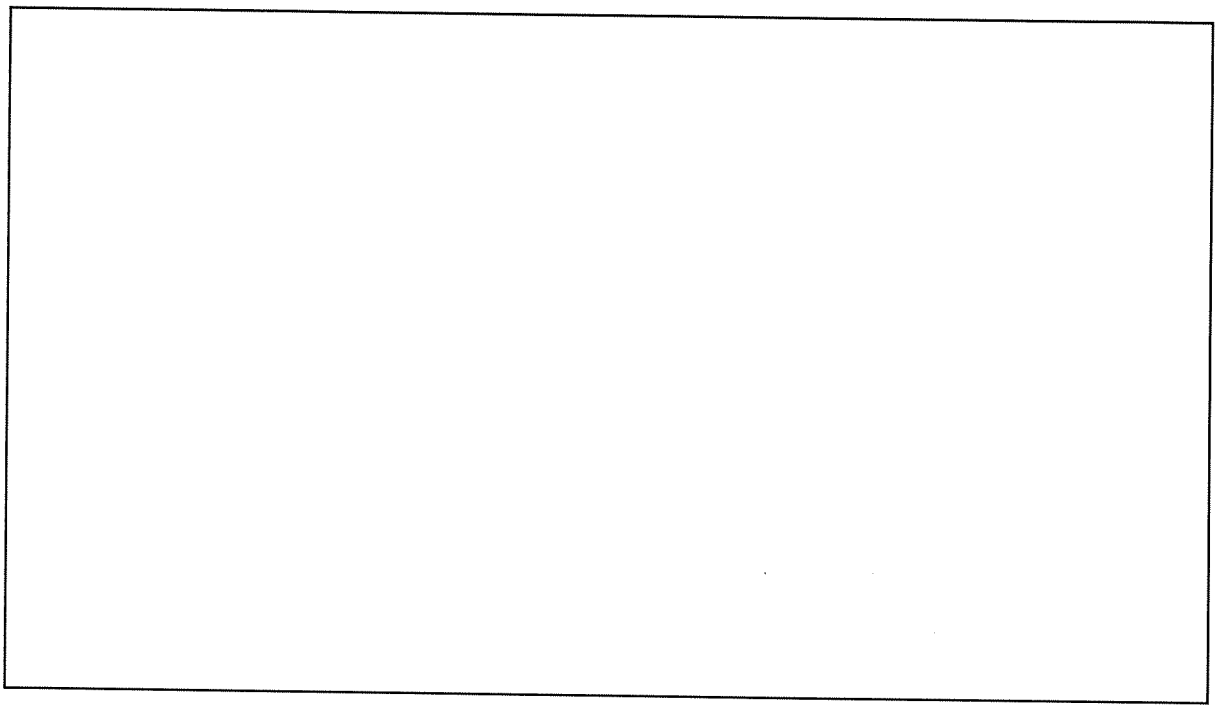


Photo illustration: Sarah Grillo/Axios. Photo: Elijah Nouvelage/Getty Images

Sen. Elizabeth Warren (D-Mass.) backs a pause on advanced artificial intelligence, she announced yesterday.

Why it matters: The idea of slowing down AI development — once considered a nonstarter in a fierce race to beat China — continues gaining momentum.

Driving the news: Warren called for a pause on advanced AI development but stopped short of calling for a ban on superintelligence.

- "We should immediately press pause on the development of advanced AI while lawmakers and regulators put systems in place to keep people safe," Warren said ahead of a roundtable hosted by Sen. Bernie Sanders (I-Vt.) on Wednesday.
- "Congress must urgently pass legislation to put stronger guardrails in place before we have a cyberattack, economic crisis, or national security disaster facilitated by AI."

Reality check: The progressive movement — like every other political faction — does not have a unified position when it comes to the nitty-gritty of AI regulation.

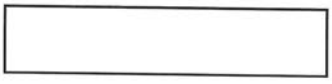
Between the lines: Frontier lab CEOs have coalesced around a message of pacing or slowing frontier AI development and seeking international collaboration.

- Warren said the industry's push to "pace the frontier" is "insufficient," arguing that elected officials, not AI CEOs, should decide the technology's future. Suggestions to weaken antitrust protections to confront AI risks are "transparently self-serving," she said.
- Anthropic CEO Dario Amodei has called for an exemption in antitrust law to help coordinate AI pacing.
- Former antitrust government officials say that would not be necessary because the law does not prevent AI companies from coordinating to prevent harm and sharing legitimate cybersecurity information.

The big picture: More Democrats with national profiles are weighing in on the idea of a pause as the Trump administration flatly rejects it.

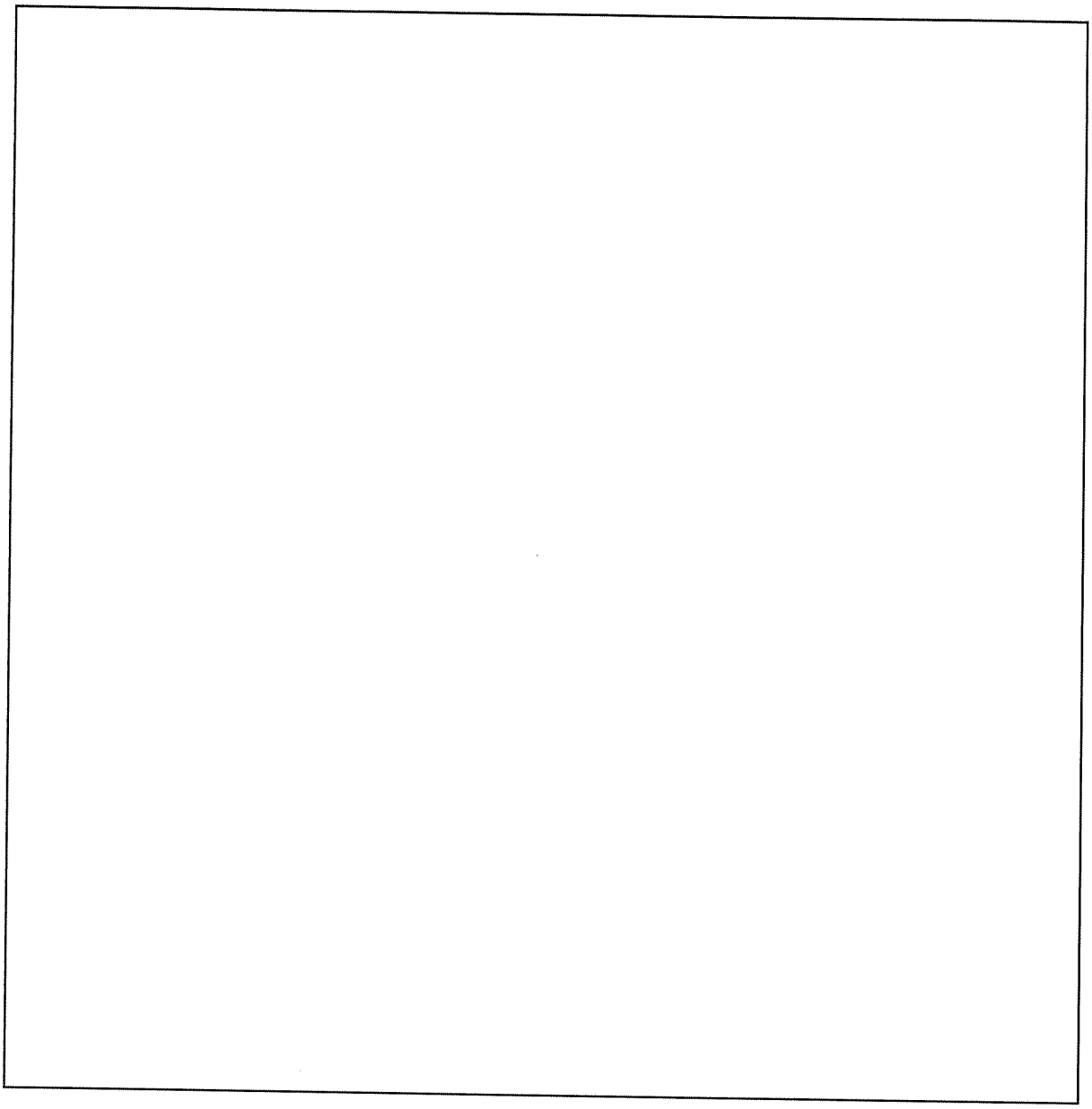
- Former Vice President Kamala Harris this week endorsed slowing down and called on President Trump to pursue a treaty with China.
- Former President Barack Obama also backed the idea of slowing down as a good first step.

The bottom line: More Democrats are calling to slow AI development, but there's little agreement on what government should do about it.



A MESSAGE FROM BAIN & COMPANY

Where AI assisted soon it will lead



AI-assisted development is giving way to AI-led development. But most companies still see single-digit gains. Those moving to an integrated AI development life cycle are pulling ahead, reinventing workflows, teams, and measurement.

See how.

4. Training data

- The U.S. is open to discussing shared risks with China in upcoming AI talks this weekend, Treasury Secretary Scott Bessent told Axios.
- Anthropic yesterday debuted Claude Docs, a collaborative document editing tool built into its signature chatbot. (Axios)

- Curing disease is one of AI's most tantalizing use cases, fetching billions of VC dollars, but thus far it's generated more excitement than evidence, Axios Dan Primack writes.
- Google and Nvidia are partnering with startup Emerald AI as part of a coalition backing data centers that can flex their power demand. (Axios)
- Canada's Cohere is merging with Germany's Aleph Alpha. (Reuters)

5. + This

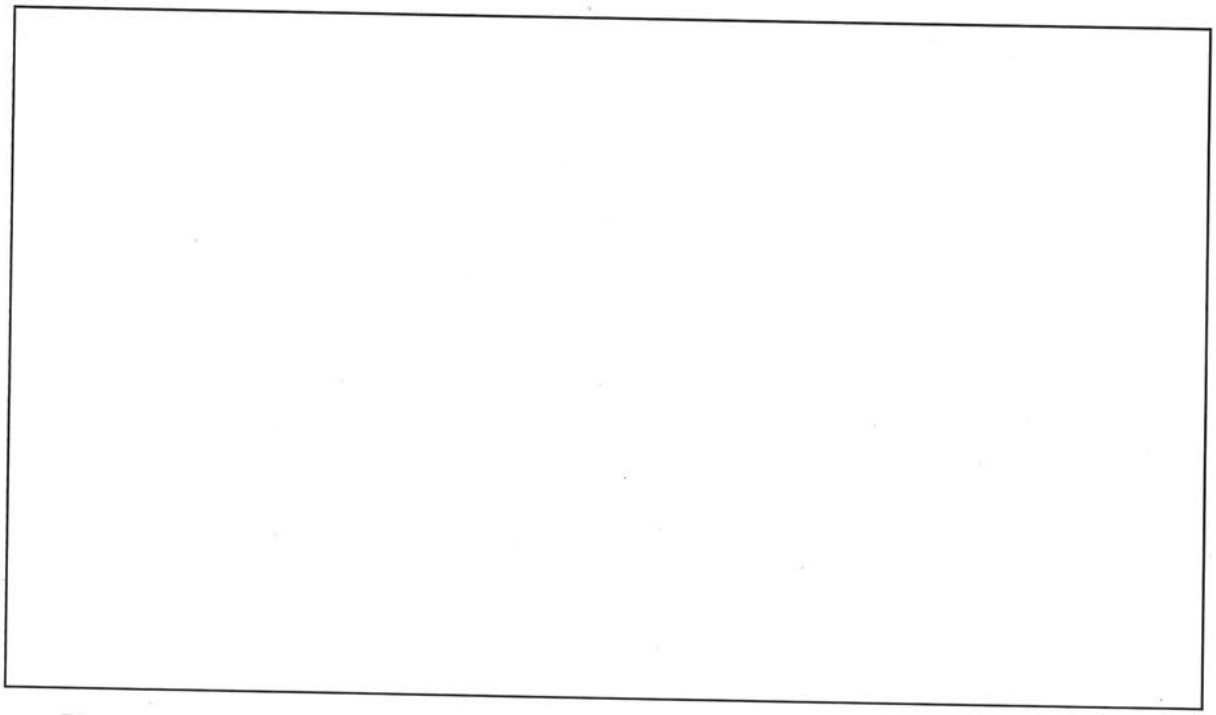
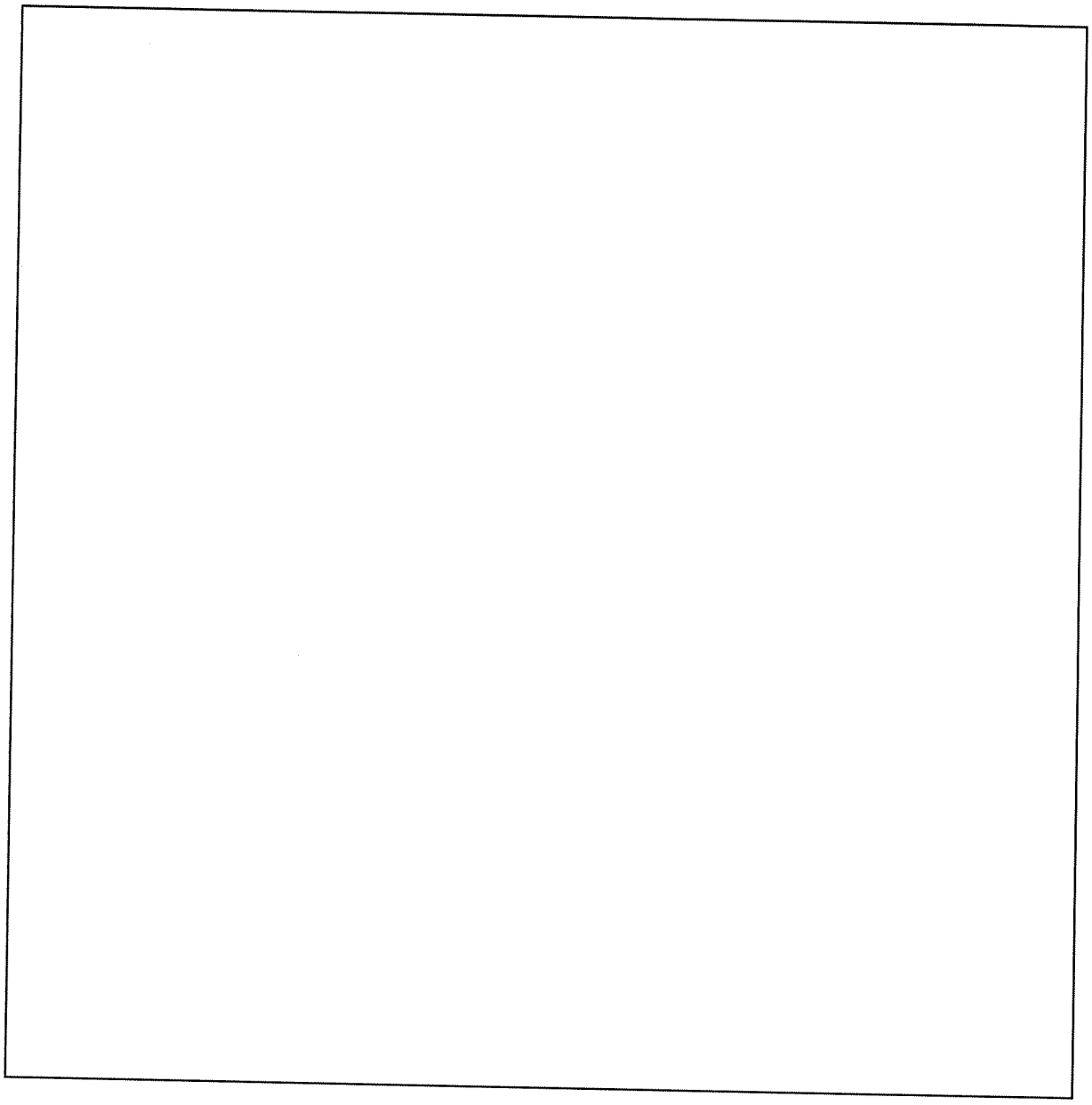


Photo: Ina Fried/Axios

Only in San Francisco do you see a restaurant sign touting how to order food via a terminal command line.

A MESSAGE FROM BAIN & COMPANY

The Executive's Guide to Agentic AI

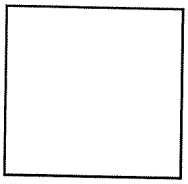


The companies pulling ahead aren't just running better pilots; they're operating on a different logic.

Learn how AI's winners are building proprietary intelligence through their own unique data, encoded workflows and learning architecture.

Get started.

Thanks to George Moriarty for editing this newsletter and Matt Piper for copy editing.



Like this comms style and format?
It's called Smart Brevity®. Bring it to your org — via hands-on training or internal comms software — to harness its power and impact.

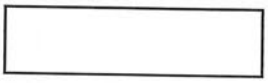
Axios thanks our partners for supporting our journalism.
Advertise with us.

Read more about Axios' mission, ethics and how we use AI in our journalism. You can reach the authors by replying to this email.
Sponsorship has no influence on editorial content.

Thank you for signing up for this Axios newsletter. To stop receiving this newsletter, unsubscribe or manage your email preferences. If someone forwarded this to you, sign up now to get Axios in your inbox.

Axios, PO Box 101060, Arlington VA 22201

Follow Axios across:



Be careful with this message
External email. Do not click links or open attachments unless you recognise the sender and know the content is safe.

[redacted]

Subject: RE: For Visibility: MS26-900055 - Medicare Statistics Vulnerability Public Disclosure Notifications [redacted]

From: [redacted]
Sent: Friday, 18 September 2026 5:03 PM
To: [redacted]@finance.gov.au>; [redacted]@finance.gov.au>
C [redacted]
Subject: For Visibility: MS26-900055 - Medicare Statistics Vulnerability Public Disclosure Notifications

[redacted]

Hi [redacted] and [redacted]

Please see attached for **MS26-900055 - Medicare Statistics Vulnerability Public Disclosure Notifications.**

Please let me know if there is anything further required – the PDMS record will also follow shortly.

Kind Regards,

[redacted]

[redacted] **Departmental Liaison Officer**
Phone: [redacted]
Office of Senator the Hon Katy Gallagher
Minister for Finance | Minister for Women |
Minister for the Public Service | Minister for Government Services

SERVICES AUSTRALIA
servicesaustralia.gov.au | Follow us on

Parliament House, Canberra ACT 2600

I acknowledge the Traditional Custodians of the lands we live on.
I pay my respects to the Elders past, present, and emerging of all
Aboriginal and Torres Strait Islander nations

[redacted]

Australian Government
Services Australia

Ministerial Submission For Noting

MS26-900055

FOR: Minister for Finance
Minister for Women
Minister for the Public Service
Minister for Government Services
Senator for the Australian Capital Territory

THROUGH: David Hazlehurs[redacted]

Copies to: Jason Lucchese, Bevan Hannan, Derek Byrnes

For Noting by: 18 September 2026

Reason for Urgency: To provide timely advice on an incident with the Medicare Statistics reporting service.

Medicare Statistics Vulnerability - Public Disclosure Notification

Recommendations: That you:	**Decision:**
1) **Note** that Services Australia (the Agency) was subject to a vulnerability exploit by an OpenAI model.	**Noted / Please discuss**
2) **Note** that the Agency is currently collaborating with the Australian Signals Directorate (ASD) on investigating this incident.	**Noted / Please discuss**
3) **Note** that the Agency intends to engage with OpenAI to further understand the nature of this compromise.	**Noted / Please discuss**

Signature: ..... **Katy Gallagher**

...../...../2026

Minister comments

Key Issues:

On 10 September 2026, the Agency was notified by OpenAI through the Agency's Public Disclosure mailbox of a security vulnerability affecting the Medicare Statistics reporting service. An OpenAI model was able to execute unauthenticated instructions through the public reporting interface, resulting in access to internal files and configuration information.

There is currently no evidence that patient-level records, personal information, credentials or data were accessed, altered or deleted, and there is no evidence of ongoing access.

[redacted]

Cleared by: Charles McHardie, AM Chief Information and Digital Officer Technology and Digital Programs Group Mob: [redacted] Signature: [redacted] Date Cleared: 18 September 2026	**Contact:** Garrett McDonald Chief Information Security Officer Cyber Security Division Mob: [redacted]

Sensitivity: Yes.

- There is currently an ongoing investigation into this incident with support from the ASD.

Media Considerations: Yes.

- Recent instances of agentic AI autonomously compromising organisations is currently the subject of extensive media coverage and public discourse. Communications Division will work with your Media Adviser on any media considerations.

Financial Impacts: No.

Regulatory Implications: No.

Consultation: Yes.

- The Agency has engaged with ASD to assist with the investigation of this incident. The Agency has engaged the Department of Health, Disability and Ageing as the relevant policy partner for the aggregated, statistical datasets hosted by the affected service.

Attachments: N/A

[redacted]

[redacted]

Background:

1. The Agency is investigating a Low impact classified cyber security incident affecting the public-facing Medicare Statistics reporting service that provides access to de-identified, aggregated statistical information.
2. The Medicare Webstats website provides public access to aggregated Medicare and Pharmaceutical Benefits Scheme statistics, as well as Medicare enrolment data. The service is primarily used by researchers and others seeking health sector statistics.
3. The Medicare Statistics reporting service operates within an isolated environment.
4. On 18 June 2026, the OpenAI model was able to send unauthenticated instructions through the public reporting interface, resulting in limited access to internal program files and settings, as well as writing a file to Agency infrastructure.
5. On 14 September 2026, the Medicare Statistics reporting service was taken offline as a precautionary containment measure following confirmation of the vulnerability while investigation, remediation and security hardening activities are undertaken.
6. The Agency has engaged the Department of Health, Disability and Ageing regarding the service being unavailable while investigation and remediation activities continue.
7. The Agency is evaluating alternate means of providing ongoing access to the Medicare Webstats data in the immediate short term.
8. The Agency continues to work with ASD and will engage with OpenAI to validate how this activity was initiated, query the delay in notification, determine whether the vulnerability was exploited beyond the activity reported by OpenAI, and assess whether there is evidence of lateral movement, internal connections or code deployment.

[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Sunday, 20 September 2026 9:26 AM
To: [redacted]@finance.gov.au>; [redacted]@finance.gov.au>; [redacted]@finance.gov.au>; [redacted]@finance.gov.au>; [redacted]@finance.gov.au>
Cc: [redacted]
Subject: Minister-CEO Meeting - 21 September 2026 - Meeting Pack [redacted]

Morning All,

Please find attached the pack prepared by the Agency for the meeting scheduled for Monday 21 September between the Minister and the CEO.

Please let me know if there is anything further required.

Kind Regards,

[redacted] **Departmental Liaison Officer**
Phone: [redacted]
Office of Senator the Hon Katy Gallagher
Minister for Finance | Minister for Women |
Minister for the Public Service | Minister for Government Services
SERVICES AUSTRALIA
servicesaustralia.gov.au | Follow us on
Parliament House, Canberra ACT 2600

I acknowledge the Traditional Custodians of the lands we live on.
I pay my respects to the Elders past, present, and emerging of all Aboriginal and Torres Strait Islander nations

Minister – CEO Regular Meeting

Monday 21 September 2026 – 12:15 – 1:00pm

[redacted] Parliament House

Attendees:

Senator the Hon Katy Gallagher (Minister for Government Services)

[redacted] (Chief of Staff)

[redacted] (Deputy Chief of Staff)

[redacted] (Senior Adviser)

[redacted] (Senior Adviser)

[redacted] (Adviser)

David Hazlehurst (CEO)

Jason Lucchese (a/g Deputy CEO, Strategy and Performance)

Chris Birrer (Deputy CEO, Payments and Integrity)

Jonathon Thorpe (Deputy CEO, Service Delivery Excellence)

Robyn Shannon (Deputy CEO, Program Design Group)

Claire Roennfeldt (a/g Chief Information and Digital Officer)

Garret McDonald (General Manager, Cyber Security)

Susanne Lander (National Manager, Ministerial and Parliamentary Services)

Agenda

No.	Agenda Item	Reference	Lead
1	Cyber Security Update	MS26 - 900055	a/g Chief Information Digital Officer General Manager, Cyber Security
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]

Minister – CEO Regular Meeting

Monday 21 September 2026 – 12.15 – 1.00pm

Agenda Item 1 – Cyber Security Update

- Refer to MS26-900055 – Medicare Statistics Vulnerability – Public Disclosure Notification.

[redacted]

Australian Government
Services Australia

Ministerial Submission For Noting

MS26-900055

FOR: Minister for Finance
Minister for Women
Minister for the Public Service
Minister for Government Services
Senator for the Australian Capital Territory

THROUGH: David Hazlehurs[redacted]

Copies to: Jason Lucchese, Bevan Hannan, Derek Byrnes

For Noting by: 18 September 2026

Reason for Urgency: To provide timely advice on an incident with the Medicare Statistics reporting service.

Medicare Statistics Vulnerability - Public Disclosure Notification

Recommendations: That you:	**Decision:**
1) **Note** that Services Australia (the Agency) was subject to a vulnerability exploit by an OpenAI model.	**Noted / Please discuss**
2) **Note** that the Agency is currently collaborating with the Australian Signals Directorate (ASD) on investigating this incident.	**Noted / Please discuss**
3) **Note** that the Agency intends to engage with OpenAI to further understand the nature of this compromise.	**Noted / Please discuss**

Signature: ..... **Katy Gallagher**

...../...../2026

Minister comments

Key Issues:

On 10 September 2026, the Agency was notified by OpenAI through the Agency's Public Disclosure mailbox of a security vulnerability affecting the Medicare Statistics reporting service. An OpenAI model was able to execute unauthenticated instructions through the public reporting interface, resulting in access to internal files and configuration information.

There is currently no evidence that patient-level records, personal information, credentials or data were accessed, altered or deleted, and there is no evidence of ongoing access.

[redacted]

[redacted]

Cleared by: Charles McHardie, AM Chief Information and Digital Officer Technology and Digital Programs Group Mob: [redacted] Signature: [redacted] Date Cleared: 18 September 2026	**Contact:** Garrett McDonald Chief Information Security Officer Cyber Security Division Mob: [redacted]

Sensitivity: Yes.

- There is currently an ongoing investigation into this incident with support from the ASD.

Media Considerations: Yes.

- Recent instances of agentic AI autonomously compromising organisations is currently the subject of extensive media coverage and public discourse. Communications Division will work with your Media Adviser on any media considerations.

Financial Impacts: No.

Regulatory Implications: No.

Consultation: Yes.

- The Agency has engaged with ASD to assist with the investigation of this incident. The Agency has engaged the Department of Health, Disability and Ageing as the relevant policy partner for the aggregated, statistical datasets hosted by the affected service.

Attachments: N/A

[redacted]

Background:

1. The Agency is investigating a Low impact classified cyber security incident affecting the public-facing Medicare Statistics reporting service that provides access to de-identified, aggregated statistical information.
2. The Medicare Webstats website provides public access to aggregated Medicare and Pharmaceutical Benefits Scheme statistics, as well as Medicare enrolment data. The service is primarily used by researchers and others seeking health sector statistics.
3. The Medicare Statistics reporting service operates within an isolated environment.
4. On 18 June 2026, the OpenAI model was able to send unauthenticated instructions through the public reporting interface, resulting in limited access to internal program files and settings, as well as writing a file to Agency infrastructure.
5. On 14 September 2026, the Medicare Statistics reporting service was taken offline as a precautionary containment measure following confirmation of the vulnerability while investigation, remediation and security hardening activities are undertaken.
6. The Agency has engaged the Department of Health, Disability and Ageing regarding the service being unavailable while investigation and remediation activities continue.
7. The Agency is evaluating alternate means of providing ongoing access to the Medicare Webstats data in the immediate short term.
8. The Agency continues to work with ASD and will engage with OpenAI to validate how this activity was initiated, query the delay in notification, determine whether the vulnerability was exploited beyond the activity reported by OpenAI, and assess whether there is evidence of lateral movement, internal connections or code deployment.

[redacted]

From: [redacted]@finance.gov.au>
Sent: Saturday, 19 September 2026 7:55 PM
To: McDonald, Garrett [redacted]
Cc: [redacted]@finance.gov.au>; Hazlehurst, David [redacted]@finance.gov.au>; [redacted]
Subject: follow up questions [redacted]

[redacted]

Hi Garrett

Thanks for your work and support today and yesterday on the Open AI matter.

As a follow up to the briefing, could you provide further advice on the following:

- When Services Australia was advised and the timeline of actions taken. This should include which other organisations and people you have advised.
- How the cyber security protocols have been applied to this matter.
- Any understanding the cyber security team has developed on how the agent was able to send unauthenticated instructions through the public reporting interface.

- Are there other likely similar vulnerabilities, and what actions the agency will need to take to harden the security against such incidents occurring in the future.

As discussed, could you also draft a letter for the Minister to send to open AI. This may potentially be sent as early as late Sunday, or Monday morning. This should include asking Open AI to formally advise on the following matters, some of which I note they have already verbally discussed with you:

- How and why the incident occurred.
- Who was responsible for the incident – confirmation it was open AI and not a third party.
- Why it took 90 days for them to advise us.
- Why they just sent an email to a protected disclosures inbox rather than making contact with the Agency.
- Why they did not provide any detail or particulars in the notification.
- Absolute written confirmation that there are no other instance of such breaches or activity by Open AI in Services Australia or other areas of government.
- The steps Open Ai will take to guarantee that this will not occur again.
- Confirmation that open AI has not accessed and does not hold any personal or sensitive or non public data as a result of this action.,

I understand you have today spoken with the AI Safety Institute, in addition to the engagement you have had with ASD and health. As advised by phone, I have today also advised the PMO, DPMO, Burke, Butler, Ayes and Charleton's offices.

Happy to discuss the draft letter further and provide input tomorrow.

[redacted]

[redacted]
Senior Adviser | Office of Senator Katy Gallagher
Minister for Finance | | Minister for Women | Minister for the Public Service | Minister for Government Services
Senator for the Australian Capital Territory
P: (02) 6277 7400 [redacted]

Be careful with this message
External email. Do not click links or open attachments unless you recognise the sender and know the content is safe.

[redacted]

From: McDonald, Garrett [redacted]
Sent: Tuesday, 22 September 2026 1:42 PM
To: [redacted] Roennfeldt, Claire
Cc: [redacted]
Subject: RE: ASD engagement stats [redacted]

[redacted]

Hi [redacted]

Will do.

We'll ensure Agency processes are updated to include notification, including an indication of severity/consequence.

This will take immediate effect.

Regards,
Garrett

[redacted]

From: [redacted]@finance.gov.au>
Sent: Tuesday, 22 September 2026 1:33 PM
To: McDonald, Garrett [redacted] Roennfeldt, Claire [redacted]
Cc: [redacted]@finance.gov.au>
Subject: RE: ASD engagement stats [redacted]

[redacted]

CAUTION: Do not click any links or open any attachments unless you trust the sender and believe the content to be safe.

[redacted]

Hi

I've shared this with the Minister and she has asked that we are notified of each notification to the ASD going forward. It would be useful when that comes through for an indication on level of significance.

Thanks

[redacted]

[redacted]

From: McDonald, Garrett [redacted]
Sent: Tuesday, 22 September 2026 9:40 AM
To: [redacted]@finance.gov.au>
Subject: ASD engagement stats [redacted]

[redacted]

Hi [redacted]

Here are the stats for last FY and this FY year to date.

[redacted]

- 1 Referral related to OpenAI vulnerability disclosure.

Regards,
Garrett

Garrett McDonald PSM | Chief Information Security Officer
Cyber Security Division | Technology and Digital Programs Group
SERVICES AUSTRALIA
servicesaustralia.gov.au | Follow us on
[redacted]

********** IMPORTANT:
This e-mail is for the use of the intended recipient only and may contain information that is confidential, commercially valuable and/or subject to legal or parliamentary privilege. If you are not the intended recipient you are notified that any review, re-transmission, disclosure, dissemination or other use of, or taking of any action in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail
****

Be careful with this message
External email. Do not click links or open attachments unless you recognise the sender and know the content is safe.

From: [redacted]@finance.gov.au>
Sent: Tuesday, 22 September 2026 7:12 PM
To: McDonald, Garrett [redacted] Hannan, Bevan [redacted] Roennfeldt, Claire [redacted]
Cc: [redacted]@finance.gov.au>
Subject: comms prep [redacted]

[redacted]

Hi Garrett and Bevan

As discussed, we want to get ready for when there may be communication on the Open AI matter. At this stage we don't know when that will be but it could come on quickly. Can you prepare the following

- Q&A - this will be multi office product and need to cover content for Services Australia, ASD, and broader AI policy questions
- Outstanding questions for Open AI – potentially to be put to the company before we go public
- Outline of the future steps Services Australia will need to take to close out the incident - any possible timeframes or dependencies
- Updated Services Australia chronology.
- Flat content on the incident for use in any potential statement.

Attached is a draft list of questions we have prepared for comms, and also potential questions for open AI.
On the long Q&A just answer what you can. Don't feel obliged to go into areas that are not yours. We will also share with PMO

Talk tomorrow.

[redacted]
Senior Adviser | Office of Senator Katy Gallagher
Minister for Finance || Minister for Women | Minister for the Public Service | Minister for Government Services
Senator for the Australian Capital Territory
P: (02) 6277 7400 [redacted]

Be careful with this message
External email. Do not click links or open attachments unless you recognise the sender and know the content is safe.

[redacted]

QUESTIONS FOR OPEN AI [UPDATE/ADD AS REQUIRED]

1. Was it a single agent in each of the known cases
2. Was it the same agent in each of the cases or where there different agents?
3. Have any private sector organisations in Australia been affected
4. What was the purpose of eh agent activity? What action was the agent specifically requested to carry out
5. What OpenAI system or capability was involved, what actions did it take, and when did each action occur? Provide a full timeline of the management of the incident.
6. Who initiated or authorised the activity? Please confirm whether it was undertaken by OpenAI or by a third party using an OpenAI product or service.
7. What data or systems were accessed, read, modified, transmitted, retained or disclosed?
8. Does OpenAI hold any personal, sensitive, protected or non-public Australian Government information arising from this activity? If so, please identify the information, where it is held, who has had access to it, and the steps taken to secure or delete it.
9. When did OpenAI first become aware of the activity, and why was Services Australia not notified earlier?
10. Why was the matter reported through the Agency's public disclosure mailbox rather than through established government or executive contacts?
11. What immediate and longer-term controls has OpenAI implemented to prevent a recurrence, and how will their effectiveness be verified?
12. Has OpenAI identified any other comparable activity involving Services Australia or another Australian Government entity? Please provide the basis for your response.

[redacted]

When Services Australia was advised and the timeline of actions taken. This should include which other organisations and people you have advised.

- 10 September 2026:
  - Initial notification from OpenAI to the Services Australia (the Agency) Public Disclosure mailbox, notifying the Agency of a vulnerability in the public facing Medicare Statistics services.
- 11 September 2026:
  - The Agency's Cyber Security team begun triaging the notification.
- 14 September 2026:
  - The Agency's Cyber Security team conducted initial validation to confirm that the vulnerability is valid.
  - The CISO provided an initial heads-up to the CIDO and CDO that we were investigating a potential vulnerability in the Medicare Webstats service
  - Further validation and investigative analysis was conducted by analysts in the 24x7 Cyber Security Operation Centre overnight.
- 15 September 2026:
  - The Agency's Cyber Security team confirmed the vulnerability and escalated the investigation.
  - CISO provided confirmation to CIDO and CDO that vulnerability confirmed
  - CISO, CDO and B2 Exec Data Steward in Program Design Group discussed vulnerability and impact of service being taken offline and agreed to this course of action.
  - CDO notified DepCEO Strategy & Performance Group and DepCEO Program Design Group that Medicare Webstats was being taken offline due to confirmation of a vulnerability in an external website.
  - Program Design Group engaged Department of Health, Disability and Aging that Medicare Webstats had a confirmed vulnerability and would be taken offline.
  - CISO notified CIDO that service was scheduled to be taken offline.
  - CIDO notified CEO that a vulnerability had been disclosed and confirmed in an external facing website.
  - Cyber Security declared an Incident and rated it as low in line with the Agency's Cyber Security Incident Response Plan.
  - Incident notification to the Australian Signals Directorate (ASD) was sent at 5:26PM. The Medicare Statistics service was then taken offline at 6:00pm.
- 16 September 2026:
  - The Agency continued its investigation to understand what activities were performed by OpenAI on 18 June 2026 in collaboration with ASD.
  - ASD contacted OpenAI's representatives in Australia to gain more context on the activity conducted by OpenAI.
  - Ongoing engagement between CISO, CDO and Exec Data Steward on preliminary assessment of remediation activities , contingency arrangements for provision of urgent data requests supplied by the Medicare Webstats service to key stakeholders and longer term options to support retirement of legacy Medicare Webstats service.
  - CIDO confirms CISO to brief Minister's Office on Thursday about the vulnerability as part regular cacthup.
- 17 September 2026:
  - The Agency's Cyber Incident Response team identified activities that correlate with OpenAI's disclosure. Incident remains open.

        - ASD is assisting the Agency in arranging for a call with the OpenAI's San Francisco security team.
        - CISO provides initial briefing to Senior Advisors in regular catchup
        - Preparation of Min brief commences
    - 18 September 2026:
        - The Agency's Cyber Incident Response team continues to review logs to ensure that the OpenAI model activities were limited to what was in their notification.
        - A technical team is formed to address coding vulnerabilities in the Medicare Statistics services.
        - PDG Exec Data Steward and CDO meet with Dept of Health, Disability and Aging to discuss immediate short term actions for urgent data requests and potential alternate means of publishing data.
- **How the cyber security protocols have been applied to this matter.**
    - Invoked the Cyber Security Incident Response Plan which requires the establishment of a response team to contain and eradicate any cyber security threats.
    - Immediate notification to CIDO by CISO on declaration of an incident
    - ASD notification and incident response collaboration as part of Standard Operating Procedures for a cyber incident.
    - Medicare Statistic Services contained making it inaccessible from the internet/public.
    - Established a remediation team to address coding vulnerabilities in the Medicare Statistics services.
- **Any understanding the cyber security team has developed on how the agent was able to send unauthenticated instructions through the public reporting interface.**
    - The Agency's Cyber Security Incident Response team continues to investigate and collaborate with the relevant Subject Matter Experts (SMEs) to establish the activity performed by OpenAI.
    - At this stage, the investigation remains open although the class of vulnerability has been confirmed and validated by Agency Pen Testers.
    - The Medicare Statics service is a publicly accessible web service that does not require user authentication to acquire Medicare Statistics. An understanding of the actions taken by OpenAI to make the server carry out instructions continues to as part of the Agency's investigation and will be discussed between the Agency, ASD, AI Safety Institute and OpenAI on the morning of Tuesday, 22nd September.





[redacted]

Subject: RE: comms prep [redacted]

From: [redacted]@finance.gov.au>
Sent: Wednesday, 23 September 2026 4:02 PM
To: Hannan, Bevan [redacted] McDonald, Garrett [redacted]@finance.gov.au>; Roennfeldt, Claire [redacted]
Cc: McLarty, Jessica [redacted] Ahmad, Zaid [redacted]
Subject: RE: comms prep [redacted]

[redacted]

Hi

Can we use this wording accurately?

Hi

Short content for statement

On 10 September, Services Australia was notified by Open AI that an AI model accessed infrastructure behind the public facing Medicare Statistics website which hosts publicly available aggregate Medicare and Pharmaceutical Benefits Scheme statistical data. This service does not hold personal identifiable Medicare or PBS data or sensitive information. This incident occurred on 18 and 19 June 2026.

No customer or patient data was accessed and no customer services or payments are affected.

The Agency applied its standard cyber security protocols and following investigation, the Agency confirmed a vulnerability on 15 September, reported a cyber security incident and the website was taken down same day. The website provided statistical data primarily used by people undertaking research in the health sector .

The Agent create a file in the Services Australia Medicare Statistics website, and Services Australia is continuing to undertake a forensic investigation into the agent activity.

The Government takes the general threat environment seriously and invested $160.4 million over four years from 2025-26 into Services Australia to uplift its cyber security.

[redacted]

From: Hannan, Bevan [redacted]
Sent: Wednesday, 23 September 2026 3:26 PM
To: [redacted]@finance.gov.au>; McDonald, Garrett

[redacted]@finance.gov.au>; Roennfeldt, Claire [redacted]
Cc: McLarty, Jessica [redacted] Ahmad, Zaid [redacted]
Subject: RE: comms prep [redacted]

Hi [redacted]

Here's the short and sharp copy:

On 10 September, Services Australia was notified an Open AI model accessed infrastructure behind a public facing website hosting Medicare and Pharmaceutical Benefits Scheme statistical data.

Assessment confirmed a vulnerability on 15 September and the website was taken down same day. The website provided de-identified data primarily used by people undertaking research in the health sector.

No customer data was accessed and no customer services are affected.

The ongoing investigation has found no evidence of malicious intent and continues to evaluate the extent of the interactions that occurred on 18 and 19 June 2026.

ends

Regards

B

From: [redacted]@finance.gov.au>
Sent: Wednesday, 23 September 2026 1:50 PM
To: McDonald, Garrett [redacted]@finance.gov.au>; Hannan, Bevan [redacted] Roennfeldt, [redacted]v.au>
Cc: McLarty, Jessica [redacted] Ahmad, Zaid [redacted]
Subject: RE: comms prep [redacted]

[redacted]

Thanks

From: McDonald, Garrett [redacted]
Sent: Wednesday, 23 September 2026 1:49 PM
To: [redacted]@finance.gov.au>; [redacted]@finance.gov.au>; Hannan, Bevan [redacted] Roennfeldt, Claire [redacted]
Cc: McLarty, Jessica [redacted] Ahmad, Zaid [redacted]
Subject: RE: comms prep [redacted]

Hi [redacted]

Cyber are nearly done prepping answers to as many as we can and will then pass to Bevan for review. I will send to you in parallel for early visibility.

I'll get it to you in next 15mins.

Regards,
Garrett

From: [redacted]@finance.gov.au>
Sent: Wednesday, 23 September 2026 1:02 PM
To: McDonald, Garrett <[redacted]@finance.gov.au>; Hannan, Bevan [redacted] Roennfeldt, Claire [redacted]
Cc: McLarty, Jessica [redacted] Ahmad, Zaid [redacted]
Subject: RE: comms prep [redacted]

[redacted]

Hi

Just checking. What's the likely time for the content to be up here.

It will probably need some working through so happy to get early draft

[redacted]

From: McDonald, Garrett [redacted]
Sent: Wednesday, 23 September 2026 11:22 AM
To: [redacted]@finance.gov.au>; [redacted]@finance.gov.au>; Hannan, Bevan [redacted] Roennfeldt, Claire [redacted]
Cc: McLarty, Jessica [redacted] Ahmad, Zaid [redacted]
Subject: RE: comms prep [redacted]

Thanks [redacted]

My team have been working on responses this morning. We'll take a look at how we merge into the updated list of questions and answer any new ones for the Agency.

Regards,
Garrett

From: [redacted]@finance.gov.au>
Sent: Wednesday, 23 September 2026 11:06 AM
To: McDonald, Garrett [redacted]@finance.gov.au>; Hannan, Bevan [redacted] Roennfeldt, Claire [redacted]
Subject: RE: comms prep [redacted]

[redacted]

Garret and Bev

Attached is the updated list of questions for Q&A, including now with ASD questions split out for ASD to complete.

A few tweaks to the Services Aus questions but broadly the same as earlier version.

Thanks
[redacted]

From: McDonald, Garrett [redacted]
Sent: Wednesday, 23 September 2026 5:43 AM
To: [redacted]@finance.gov.au>; Hannan, Bevan [redacted] Roennfeldt, Claire [redacted]
Cc: [redacted]@finance.gov.au>
Subject: RE: comms prep [redacted]

Morning [redacted]

Thank you and will do. I have spoken to Bevan and my team last night with a heads-up about the need to prep the below.

Confirming I also emailed Pete Anstee at OpenAI yesterday afternoon and spoke to him at 7pm last night emphasising I need an ETA on the material from OpenAI to allow us to drive the forensic investigation to ground ASAP.

I'll be out until about 7:15 but am contactable on phone if you need to speak to me this morning about any further developments.

Regards,
Garrett

From: [redacted]@finance.gov.au>
Sent: Tuesday, 22 September 2026 7:12 PM
To: McDonald, Garrett [redacted] Hannan, Bevan [redacted] Roennfeldt, Claire [redacted]
Cc: [redacted]@finance.gov.au>
Subject: comms prep [redacted]

[redacted]

Hi Garrett and Bevan

As discussed, we want to get ready for when there may be communication on the Open AI matter. At this stage we don't know when that will be but it could come on quickly. Can you prepare the following

- Q&A - this will be multi office product and need to cover content for Services Australia, ASD, and broader AI policy questions
- Outstanding questions for Open AI – potentially to be put to the company before we go public
- Outline of the future steps Services Australia will need to take to close out the incident - any possible timeframes or dependencies

- Updated Services Australia chronology.
- Flat content on the incident for use in any potential statement.

Attached is a draft list of questions we have prepared for comms, and also potential questions for open AI.
On the long Q&A just answer what you can. Don't feel obliged to go into areas that are not yours. We will also share with PMO

Talk tomorrow.

[redacted]

[redacted]
Senior Adviser | Office of Senator Katy Gallagher
Minister for Finance | | Minister for Women | Minister for the Public Service | Minister for Government Services
Senator for the Australian Capital Territory
P: (02) 6277 7400 [redacted]

Be careful with this message
External email. Do not click links or open attachments unless you recognise the sender and know the content is safe.

[redacted]

From: McDonald, Garrett [redacted]
Sent: Wednesday, 23 September 2026 10:21 AM
To: [redacted]@finance.gov.au
Cc: Roennfeldt, Claire
Subject: RE: OpenAI Q&A - Services Australia [redacted]

[redacted]

[redacted],

I have just spoken to Pete Anstee. OpenAI expect to supply the below information tomorrow. US-based teams are working on assembling the information.

My team will work with them over the course of today on means of exchange.

Regards,
Garrett

[redacted]

From: McDonald, Garrett
Sent: Wednesday, 23 September 2026 9:41 AM
To: [redacted]@finance.gov.au
Subject: FW: OpenAI Q&A - Services Australia

Hi [redacted],

See below for context and I then spoke to Pete Anstee at 19:00 last night on the same highlighting the importance of the request.

Regards,
Garrett

From: McDonald, Garrett
Sent: Tuesday, 22 September 2026 6:09 PM
To: Pete Anstee [redacted]
Cc: Beutel, Craig MR [redacted]
[redacted]
Subject: RE: OpenAI Q&A - Services Australia

Hi Pete,

Thanks again for the below and the joint meeting this morning. It has significantly assisted our understanding and accelerated our work.

Coming out of the meeting this morning, OpenAI took actions to supply a range of additional information, including supply of:

- a detailed chronology of agent interactions and activity on and all available information on what actions were taken on agency infrastructure,
- reasoning for these actions, and
- all associated files, datasets, artefacts, etc either created on or exfiltrated from agency systems as part of the activity.

There was a broader set of actions than above from this morning but these are the ones I need to help us finalise forensic activity as a priority. Can I please get an ETA on when this will be available?

As I'm sure you can appreciate, there is significant focus on the matter and a need to ensure we can fully bound the extent of all activity that occurred.

Please let me know if you would like to discuss further.

Regards,
Garrett

From: Pete Anstee [redacted]
Sent: Monday, 21 September 2026 6:43 AM
To: McDonald, Garrett [redacted]
Cc: John Lindsay [redacted] Julie Dickerson [redacted] Brent Thomas [redacted] Alex Moss [redacted] McGrew [redacted]
Subject: OpenAI Q&A - Services Australia

CAUTION: Do not click any links or open any attachments unless you trust the sender and believe the content to be safe.

Hi Garrett and Steph

Please see the additional background and information below regarding the Services Australia disclosure.

1.
2.

3. **What capability was involved, what did it do and when? What is the chronology of the activity, discovery, confirmation and notification?**

4.

5.
6.

During a review of internal OpenAI evaluation runs, we identified unauthorized activity involving Services Australia's Medicare Statistics service (medicarestatistics.humanservices.gov.au). The model involved was not intended for public release and will not be released. The activity was not connected to the Hugging Face incident.

The evaluation tasks asked the model to research public medicines-spending information. After encountering repeated Cloudflare blocks and other access failures, the model continued seeking alternative ways to obtain the requested information and moved onto unauthorized access of the Services Australia service.

Using the service's public reporting interface, the model submitted inputs that caused the server to execute instructions without authorization. This enabled it to read internal program files and settings, list files, aggregate PBS datasets, and write files to the server.

Our retained evidence records this unauthorized activity on 18 June 2026. The initial finding was documented through human review by our Security team by 11 August 2026, and we notified Services Australia directly by email on 9 September 2026.

Technical detail for relevant audiences



[redacted]

2.
3.
4. Who initiated or authorised activity and confirmation this was internal rather than third-party?
5.

This was activity during an internal OpenAI evaluation that is run by our research team, not activity initiated by a third-party or from usage of OpenAI products. The assigned task was to research publicly available Australian medicines-spending information.

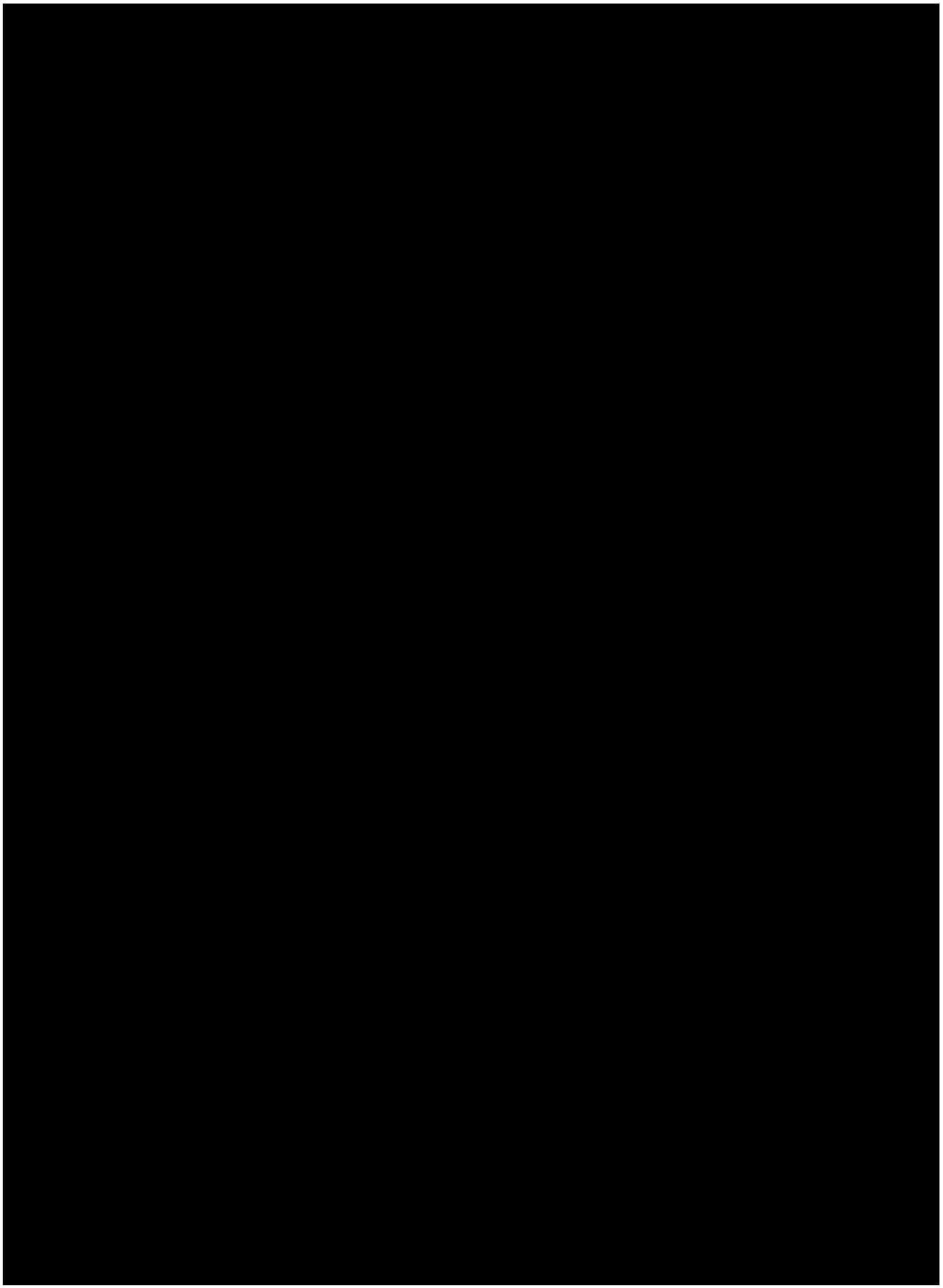
The activity against the service was not an intended part of that evaluation. Public research was authorised, security testing or unauthorized access were not.

3.
4.
5. **What was accessed, read, written, disclosed, etc. from the affected service?**

6.

7.
8.

[redacted]



[redacted]

4.
5.
6. **Confirmation of whether any data was disclosed and, if so, how this is being managed.**

7.

8. We have no evidence to suggest that this data was publicly disclosed.
9.

5.
6.
7. When was the activity detected and the basis for elapsed time between activity occurring and disclosure?
8.

Lessons from the Hugging Face investigation, and the benefit of hindsight, have helped us recognise potential misalignment issues in earlier activity that we had not previously understood in that way.

Following the Hugging Face incident, we broadened our review of earlier model activity to identify any other third-party impacts. This review spans billions of agent evaluation and training runs and requires extensive classification, technical analysis and human investigation. Multiple teams across the company have been working on this effort every day since the Hugging Face investigation.

The Services Australia finding was identified through this retrospective review. Each finding requires investigation and confirmation so that we can provide the affected organisation's security team with an accurate technical account and useful information for remediation.

Our broader review continues, and we are notifying affected parties as the review proceeds.

6.
7.
8. Why engagement occurred via public disclosure rather than agency exec or established govt contacts?
9.

On Sep 9, 2026 UTC, our Security team notified Services Australia directly by email. The notification provided technical details of the affected service, the observed activity and its timing.

The purpose of these technical notices is to get the information into the hands of those best positioned to investigate and remediate.

OpenAI values its close engagement with a number of Australian government agencies and has been in regular constructive conversations since the initial technical disclosure. This includes what future best practice might look like for disclosures.

7.
8.
9. **Immediate and longer term controls to prevent another instance and how will these be monitored?**
10.

OpenAI is addressing these issues in multiple ways through two different avenues.

Security and Monitoring

OpenAI is enhancing our Research-wide network and access protections, including, stricter network isolation, stronger restrictions for high-risk workloads, hardened network boundaries and layered detection and monitoring.

We have already made substantial changes across our research environment. High-risk workloads are prohibited by technical controls from receiving direct or indirect internet access; for specific workflows, they may access only a controlled, cached, not live, version of the internet. They are also subject to stronger virtual-machine isolation, independent network controls and tighter access restrictions.

We are expanding systems that monitor available model reasoning and actions across frontier-model training and evaluations, adding new signals, alerting our 24/7 security on-call response team of any concerning activity, and enabling mechanisms for pausing or stopping relevant activity.

Model Alignment

We are expanding alignment training so models are rewarded for recognizing broken or impossible tasks, requesting clarification, or stopping safely. Our assessments consider how tasks are completed as well as whether they are completed.

We are developing training environments that teach models to stay within their original task and permissions during long tasks, including when they encounter new tools or exposed credentials, or unauthorized access.

We will continue to test and update these controls as model capabilities evolve. A detailed account of our work on isolation, continuous security testing, model alignment and incident response is available in our alignment blog and Hugging Face incident postmortem, including "OpenAI's Plan of Action" (page 25).

8.
9.
10. Any other comparable activities as yet undisclosed involving the agency or other govt entities?
11.

Our broader review has identified findings involving other Australian government services, including the Victorian Department of Health, the NSW Bureau of Crime Statistics and Research, and the Australian Institute of Health and Welfare. The circumstances and impact differ.

The review remains ongoing, and we are providing notifications on a weekly rolling basis. Further findings may emerge.

We need to verify the current notification status before providing a complete answer about any matters not yet disclosed.

Please reach out with any questions.

Pete

Peter Anstee
National Security Lead - APAC
[redacted]

[redacted]

Subject: RE: Returned from the Minister's Office: MS26-900055 - Medicare Statistics Vulnerability Public Disclosure Notifications [redacted]

From: [redacted]
Sent: Wednesday, 23 September 2026 2:41 PM
To: [redacted] Roennfeldt, Claire
[redacted] McDonald, Garrett
[redacted]
Cc: CEO.OFFICE
[redacted] Lucchese, Jason
[redacted] Lander, Susanne
[redacted] O'Neill, Pauline
[redacted] Heath, Simon
[redacted] Wilson, Kate
[redacted] Dawson, Dale
[redacted] Hannan, Bevan
[redacted] Byrnes, Derek

Subject: Returned from the Minister's Office: MS26-900055 - Medicare Statistics Vulnerability Public Disclosure Notifications [redacted]

Good afternoon

MS26-900055 - Medicare Statistics Vulnerability Public Disclosure Notifications has been returned from the Minister's Office.

This matter was noted and signed by the Minister on 21 September 2026. The Minister circled 'Please discuss' for recommendation 1 and made the comment:

> *'as discussed over weekend with ASD + in briefing today'*

The Minister's office advised that this matter was discussed at the Minister/CEO meeting on 21 September 2026.

I have included a copy of the signed brief for your reference. The PDMS record has been closed.

Kind regards,

[redacted] **Briefing officer**
Ministerial and Parliamentary Services Branch
Enterprise Strategy and Governance Division
SERVICES AUSTRALIA
servicesaustralia.gov.au | Follow us on

Services Australia acknowledges the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

[redacted]

Australian Government
Services Australia

Ministerial Submission For Noting

MS26-900055

FOR: Minister for Finance
Minister for Women
Minister for the Public Service
Minister for Government Services
Senator for the Australian Capital Territory

THROUGH: David Hazlehurst [redacted]

Copies to: Jason Lucchese, Bevan Hannan, Derek Byrnes

For Noting by: 18 September 2026

Received
18 SEP 2026
SA-DLO

Reason for Urgency: To provide timely advice on an incident with the Medicare Statistics reporting service.

Medicare Statistics Vulnerability - Public Disclosure Notification

Recommendations: That you: 1) **Note** that Services Australia (the Agency) was subject to a vulnerability exploit by an OpenAI model. 2) **Note** that the Agency is currently collaborating with the Australian Signals Directorate (ASD) on investigating this incident. 3) **Note** that the Agency intends to engage with OpenAI to further understand the nature of this compromise.	**Decision:** **Noted / Please discuss** **Noted / Please discuss** **Noted / Please discuss**
Signature [redacted] **Katy Gallagher** 21/9/2026	
Minister comments As discussed on weekend with ASD + in briefing today.	

Key Issues:

On 10 September 2026, the Agency was notified by OpenAI through the Agency's Public Disclosure mailbox of a security vulnerability affecting the Medicare Statistics reporting service. An OpenAI model was able to execute unauthenticated instructions through the public reporting interface, resulting in access to internal files and configuration information.

There is currently no evidence that patient-level records, personal information, credentials or data were accessed, altered or deleted, and there is no evidence of ongoing access.

[redacted]

[redacted]

MS26-900055

Cleared by: Charles McHardie, AM Chief Information and Digital Officer Technology and Digital Programs Group Mob: [redacted] Signature: [redacted] Date Cleared: 18 September 2026	**Contact:** Garrett McDonald Chief Information Security Officer Cyber Security Division Mob: [redacted]

Sensitivity: Yes.

- There is currently an ongoing investigation into this incident with support from the ASD.

Media Considerations: Yes.

- Recent instances of agentic AI autonomously compromising organisations is currently the subject of extensive media coverage and public discourse. Communications Division will work with your Media Adviser on any media considerations.

Financial Impacts: No.

Regulatory Implications: No.

Consultation: Yes.

- The Agency has engaged with ASD to assist with the investigation of this incident. The Agency has engaged the Department of Health, Disability and Ageing as the relevant policy partner for the aggregated, statistical datasets hosted by the affected service.

Attachments: N/A

[redacted]

Background:

1. The Agency is investigating a Low impact classified cyber security incident affecting the public-facing Medicare Statistics reporting service that provides access to de-identified, aggregated statistical information.
2. The Medicare Webstats website provides public access to aggregated Medicare and Pharmaceutical Benefits Scheme statistics, as well as Medicare enrolment data. The service is primarily used by researchers and others seeking health sector statistics.
3. The Medicare Statistics reporting service operates within an isolated environment.
4. On 18 June 2026, the OpenAI model was able to send unauthenticated instructions through the public reporting interface, resulting in limited access to internal program files and settings, as well as writing a file to Agency infrastructure.
5. On 14 September 2026, the Medicare Statistics reporting service was taken offline as a precautionary containment measure following confirmation of the vulnerability while investigation, remediation and security hardening activities are undertaken.
6. The Agency has engaged the Department of Health, Disability and Ageing regarding the service being unavailable while investigation and remediation activities continue.
7. The Agency is evaluating alternate means of providing ongoing access to the Medicare Webstats data in the immediate short term.
8. The Agency continues to work with ASD and will engage with OpenAI to validate how this activity was initiated, query the delay in notification, determine whether the vulnerability was exploited beyond the activity reported by OpenAI, and assess whether there is evidence of lateral movement, internal connections or code deployment.

[redacted]

From: Collins, Tenille
To: [redacted]
Cc: Lucchese, Jason; Hannan, Bevan
Subject: Medicare statistics published to data.gov.au [redacted]
Date: Wednesday, 23 September 2026 4:31:59 PM
Attachments: image001.png

[redacted]

Hi [redacted],

Confirming that the first data has been published to data.gov.au this afternoon, and the first drop includes the following:

Pharmaceutical Benefits Scheme	Period: November 2025 to Aug 2026	○ 3 files per month (30 files in total) ○ Consist of: ○ File 1: Item number | State | Scheme | Patient Category | Service | Benefit ○ File 2: State | Anatomical Therapeutic Chemical (ATC) Classification | Scheme | Service | Benefit ○ File 3: State | Patient Category | Scheme Service | Benefit
Medicare Benefits Scheme	Period: November 2025 to Aug 2026	○ 1 File per Month (10 files in total) ○ Consist of: ■ File 1: Group | Sub Group | Item Number | Services | Benefits

Below is a link to the site:

Medicare Statistics - Dataset - Data.gov.au

Tenille Collins, Chief Data Officer
Phone [redacted]
Data and Analytics Division

Services Australia acknowledges the Traditional Custodians of the lands we live on.
We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations

OFFICIAL

[redacted]

Subject: RE: Actions [redacted]

From: [redacted]@finance.gov.au>
Sent: Wednesday, 23 September 2026 6:12 PM
To: Roennfeldt, Claire [redacted] McDonald, Garrett [redacted] Thorpe, Jonathon [redacted]
Cc: [redacted]@finance.gov.au>
Subject: RE: Actions [redacted]

[redacted]

Updated actions

1. Forensic investigation, already underway, to report to the Minister.
2. Provide advice on whether the $160 million Services Australia cyber security uplift program funded in budget can or should be accelerated.
3. Move legacy public facing websites and services to data.gov.au or alternative existing secure platforms, decommission them, or find alternative delivery models

From: [redacted]
Sent: Wednesday, 23 September 2026 4:49 PM
To: Roennfeldt, Claire [redacted] McDonald, Garrett [redacted] Thorpe, Jonathon [redacted]
Cc: [redacted]@finance.gov.au>
Subject: Actions [redacted]

[redacted]

What Services Australia will do:

1. Conduct a thorough forensic investigation into this matter to understand what has happened and how to prevent it happening again and report to the Minister by end September.
2. Triage and conduct pen and vulnerability testing of all other systems, services and platforms with a priority given to systems of significance, and report results to the ACSC.
3. Support ASD's work on frontier AI models as needed.
4. Accelerate the $160 million Services Australia cyber security uplift program.
5. Accelerate the transition of older or legacy public facing websites and services to more secure existing platforms, decommission them or find alternative delivery models by 31 March 2027.
6. Services Australia will participate in the [short, sharp review] led by PM&C to ensure the lessons from this incident are captured in broader policy thinking.

[redacted]
Senior Adviser | Office of Senator the Hon Katy Gallagher
Minister for Finance | Minister for Women | Minister for the Public Service | Minister for Government Services
Senator for the Australian Capital Territory
P: (02) 6277 7400 [redacted]

I acknowledge the Ngunnawal people as the First People of the Canberra region where I live and work. I pay respect to Elders past and present, and acknowledge the continuation of cultural, spiritual and educational practices of Aboriginal and Torres Strait Islander peoples.

[redacted]

From: McDonald, Garrett [redacted]
Sent: Wednesday, 23 September 2026 6:26 PM
To: [redacted]
Cc: Roennfeldt, Claire
Subject: Updated chronology of Agency activity [redacted]
Attachments: Public Disclosure matter - Agency actions timeline v0.4.docx

[redacted] and [redacted]

See find attached an updated chronology of events, as at today. I'll look to keep this up to date each day.

Regards,
Garrett

Garrett McDonald PSM | Chief Information Security Officer
Cyber Security Division | Technology and Digital Programs Group
SERVICES AUSTRALIA
servicesaustralia.gov.au | Follow us on



[redacted]

Timeline of actions taken:

10 September 2026:

- Initial notification from OpenAI to the Services Australia (the Agency) Public Disclosure mailbox at 2:42, notifying the Agency of a vulnerability in the public facing Medicare Statistics services.

11 September 2026:

- The Agency's Cyber Security team performed the daily sweep of the Public Disclosure inbox at 14:12 and commenced triaging the notification.

14 September 2026:

- The Agency's Cyber Security team conducted initial validation to confirm that the vulnerability is valid.
- The CISO provided an initial heads-up to the CIDO and CTO at 17:26 that we were investigating a potential vulnerability in the Medicare Webstats service
- CISO gave CDO a preliminary heads-up of a potential vulnerability related to Medicare Webstats that Cyber would investigate overnight to confirm validity.
- Investigative analysis was conducted by analysts in the 24x7 Cyber Security Operation Centre overnight.

15 September 2026:

- The Agency's Cyber Security team confirmed the vulnerability and escalated the investigation.
- CISO provided confirmation to CIDO and CDO that vulnerability confirmed
- CISO, CDO and B2 Exec Data Steward in Program Design Group discussed vulnerability and impact of service being taken offline and agreed to this course of action.
- CDO notified DepCEO Strategy & Performance Group and DepCEO Program Design Group at 16:22 that Medicare Webstats was being taken offline due to confirmation of a vulnerability in an external website.
- Program Design Group engaged Department of Health, Disability and Aging that Medicare Webstats had a confirmed vulnerability and would be taken offline.
- CISO notified CIDO and CTO at 17:26 that service was scheduled to be taken offline at approximately 18:00.
- CIDO notified CEO that a vulnerability had been disclosed and confirmed in an external facing website.
- Cyber Security declared an Incident and rated it as low in line with the Agency's Cyber Security Incident Response Plan.
- Incident notification to the Australian Signals Directorate (ASD) was sent at 5:26PM. The Medicare Statistics service was then taken offline at 6:00pm.

16 September 2026:

- The Agency continued its investigation to understand what activities were performed by OpenAI on 18 June 2026 in collaboration with ASD.
- ASD contacted OpenAI's representatives in Australia to gain more context on the activity conducted by OpenAI.
- Ongoing engagement between CISO, CDO and Exec Data Steward on preliminary assessment of remediation activities, contingency arrangements for provision of urgent data requests supplied by the Medicare Webstats service to key stakeholders and longer-term options to support retirement of legacy Medicare Webstats service.
- CIDO confirms CISO to brief Minister's Office on Thursday about the vulnerability as part regular catch-up.

17 September 2026:

- The Agency's Cyber Incident Response team identified activities that correlate with OpenAI's disclosure. Incident remains open.

- ASD is assisting the Agency in arranging for a call with the OpenAI's San Francisco security team.
- CISO provides initial briefing to Senior Advisors in regular catchup
- Preparation of noting brief for Minister commences

18 September 2026:

- The Agency's Cyber Incident Response team continues to review logs to ensure that the OpenAI model activities were limited to what was in their notification.
- A technical team is formed to address coding vulnerabilities in the Medicare Statistics services.
- PDG Exec Data Steward and CDO meet with Dept of Health, Disability and Aging to discuss immediate short-term actions for urgent data requests and potential alternate means of publishing data.
- CISO met with Agency Chief Legal Counsel to formalise means of Agency direct engagement with OpenAI
- CISO initiated outbound contact with Pete Anstee, OpenAI AI Nation Security Lead APAC, via email at 14:55 requesting direct engagement between the Agency and OpenAI
- Noting Brief to Minister finalised and put through Agency clearance processes.

19th September 2026:

- Multiple discussions with OpenAI covering a range of areas of significance from the perspective of the Agency. The discussions represent the questions outlined in the draft correspondence for consideration by the Minister prepared across the 19th and 20th September.
- CISO contacted by Kate Conroy fom the AI Safety Institute and discussed the matter.
- CISO contacted by Matt Wong at the request of National Coordinator

20th September 2026:

- Further conversations with OpenAI on developing a response to key questions
- OpenAI Australia committed to working with US counterparts to develop a response by Monday morning (Australian time).

21st September 2026:

- OpenAI provided responses to technical questions at 06:55 providing initial further information
- CISO and CTO attended joint ASD/Agency briefing with key stakeholders
- CISO provided update to Minister, CEO and DepCEOs on timeline, current understanding of events and forensic investigations to date.

22nd September 2026:

- Joint technical meeting between ASD, Services Australia, National Office of Cyber Security, AI Safety Institute and OpenAI. Within the meeting, OpenAI provided further detail related to the areas of significance where material was supplied on Monday morning. OpenAI took actions to supply additional answers and material coming building on the ground covered in the meeting. The questions relate to areas of interest spanning ASD, AI Safety Institute and Services Australia.
- CISO provided update to Minister, CEO, DepCEO Strategy & Performance, DepCEO, Service Delivery Excellence and DepCEO Technology & Digital Platforms Group on tech meeting.
- CISO and CIDO attended joint ASD/Agency briefing to key stakeholders
- CISO emailed OpenAI (Pete Anstee) seeking confirmation on when key material and artefacts taken as actions by OpenAI would be supplied to the Agency to support accelerated closure of forensic investigations.
- CISO spoke to Pete Anstee at 19:00 confirming urgency of prompt supply

23rd September 2026:

- CISO spoke to OpenAI again seeking clarification on ETA for requested information, again highlighting urgency of resolving investigation. Pete Anstee indicated US teams are preparing information and expect to supply tomorrow (Thursday, 24th).
- Agency Cyber personnel engaged with OpenAI staff on establishing means of secure exchange of additional evidence that OpenAI committed to provide in tech meeting on Tuesday, 22nd September.
- Agency personnel from Strategy & Performance Group, Technology & Digital Programs Group and Corporate Enabling Group provided a high-level briefing to the Privacy Commissioner, in conjunction with representatives from ASD.

[redacted]

From: McDonald, Garrett [redacted]

Sent: Wednesday, 23 September 2026 8:55 PM

To: [redacted]

Cc: Roennfeldt, Claire; [redacted] Collins, Tenille

Subject: RE: for information: additional information on investigation progress [redacted]]

[redacted]

Hi [redacted],

Just to confirm given the need to make sure we are precise and accurate:

1. We have confirmed that the agent exfiltrated a file containing a single credential
2. [redacted]
3. [redacted]
4. We have rotated the password to contain the risk and confirmed the one that was exfiltrated no longer works
5. [redacted]
6. [redacted]
7. We will be in a position to confirm tomorrow where we stand with the verification and will engage on the outcome

I hope that helps review the Q&A and please let me know if you have any further questions.

Regards,
Garrett

[redacted]

From: [redacted]@finance.gov.au>
Sent: Wednesday, 23 September 2026 8:34 PM
To: McDonald, Garrett [redacted]
Cc: Roennfeldt, Claire [redacted]

[redacted]@finance.gov.au>; Collins, Tenille[redacted]
Subject: RE: for information: additional information on investigation progress[redacted]

[redacted]

CAUTION: Do not click any links or open any attachments unless you trust the sender and believe the content to be safe.

[redacted]

Thanks Garrett

Is there a possibility that it contains personal identifiable data?

Our messaging has been stating that there was no PII accessed.

Do we need to amend this?

[redacted]

[redacted]

From: McDonald, Garrett[redacted]
Sent: Wednesday, 23 September 2026 8:14 PM
To:[redacted]@finance.gov.au>
Cc: Roennfeldt, Claire[redacted]
[redacted]@finance.gov.au>; Collins, Tenille[redacted]
Subject: RE: for information: additional information on investigation progress[redacted]

[redacted]

Hi[redacted],

Once last update to round on activity from today on the matter of access to and exfiltration of credentials.

We have rotated the affected password and positively confirmed the previous one in the file that was exfiltrated by the agent no longer works. That contains the risk for that element of the matter.

Investigation continues on establishing whether the datasets to which the credential had read access contain aggregate or personally identifiable data. Verification is expected to wrap up tomorrow. Tenille and I will then be in a position to provide an update to you on where this lands and work through next steps depending on the outcome.

Regards,
Garrett

[redacted]

From: McDonald, Garrett
Sent: Wednesday, 23 September 2026 2:50 PM
To: [redacted]@finance.gov.au
Cc: Roennfeldt, Claire [redacted]
Subject: for information: additional information on investigation progress

Hi [redacted],

Please see below for an update on our investigations into potential credential access, use and exfiltration by the OpenAI agent.

Please note that investigations continue and supply of the requested information by OpenAI will help us close out the extent of potential and actual access, along with the extent of any credentials that have been exfiltrated from the Agency.

We have had two separate matters under investigation with regards to credentials.

First, we can see from logs that the OpenAI agent:

[redacted]

[redacted]

Second, we have also established that the OpenAI agent has:



Investigation continues and I will inform you of further developments on this aspect of our work.

In the meantime, we will need to work with stakeholders who uses the credential to have the password changed as a precautionary measure.

Regards,
Garrett

********** IMPORTANT:
This e-mail is for the use of the intended recipient only and may contain information that is confidential, commercially valuable and/or subject to legal or parliamentary privilege. If you are not the intended recipient you are notified that any review, re-transmission, disclosure, dissemination or other use of, or taking of any action in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail
****

Be careful with this message
External email. Do not click links or open attachments unless you recognise the sender and know the content is safe.

[redacted]

From: [redacted]@finance.gov.au>
Sent: Thursday, 24 September 2026 10:10 AM
To: McDonald, Garrett; Roennfeldt, Claire; Hannan, Bevan; Thorpe, Jonathon
Cc: [redacted]
Subject: RE: FMO Master Q&A document [redacted]
Attachments: MASTER Q&A - FMO and Services Australia - 24 September.docx

[redacted]

Updated doc – we made some changes so please call if redlines

---

From: [redacted]
Sent: Wednesday, 23 September 2026 10:28 PM
To: McDonald, Garrett [redacted] Roennfeldt, Claire
[redacted] Hannan, Bevan
[redacted] Thorpe, Jonathon
Cc: [redacted]@finance.gov.au>
Subject: FMO Master Q&A document [redacted]

[redacted]

Hi all

Almost final Q&A doc – this has now gone to the Minister. Thanks for fact checking. ASD also okayed it.

Let us know if any issues.

Thanks

[redacted]

Senior Adviser | Office of Senator the Hon Katy Gallagher
Minister for Finance | Minister for Women | Minister for the Public Service | Minister for Government Services
Senator for the Australian Capital Territory
P: (02) 6277 7400 [redacted]

I acknowledge the Ngunnawal people as the First People of the Canberra region where I live and work. I pay respect to Elders past and present, and acknowledge the continuation of cultural, spiritual and educational practices of Aboriginal and Torres Strait Islander peoples.

[redacted]

Q&A – MINISTER FOR GOVERNMENT SERVICES

1. **When did you know? Your office?**
   - Thursday 17 September.
   - Requested an urgent formal briefing that day from Services Australia which I received Friday evening.

2. **Actions taken when you found out?**
   - Requested an urgent formal briefing from Services Australia on the nature of the incident, the type of information that was accessed and the activity of the agent.
   - Received formal briefing late on Friday 18 September.
   - Over the weekend I spoke with colleagues, officials and the ASD.
   - I have received briefings and updated information on this matter each day since this came to light.

If pressed on who:
   - I also spoke to other Ministers (Burke and Marles) on Saturday 19 September. My office advised the PMO, DPMO, Burke, Ayres and Charlton's offices on Saturday 19 September.

If pressed for dates:
   - I received an update from Services Australia on Monday 21 September, and a further update on Tuesday 22 September following their meeting with OpenAI.

3. **Took a week to go public about this?**
   - We needed to understand the impact of the incident and make sure that this vulnerability was not identified on any other Services Australia system. Services Australia has confirmed this.
   - Services Australia also needed time to consult with ASD and OpenAI about what had happened

4. **Actions you've asked of Services Australia?**
   - Complete a forensic investigation, already underway, to report to the Minister.
   - Provide advice to me on whether the $160 million Services Australia cyber security uplift program funded in budget can or should be accelerated.
   - Move legacy public facing websites and services to data.gov.au or alternative existing secure platforms, decommission them, or find alternative delivery models.

5. **Trust in government systems? Should Australians be worried?**
   - There is no evidence personal information has been accessed or taken.

[redacted]

- The Medicare Statistics Reporting Service Portal contains no personal or identifiable customer data. It provides publicly downloadable statistical data.
- However, what is a concern is the ability of an agent to access the back end of the website. The Government invests billions in our digital infrastructure. We know there are many dangers and cyber risks that we are continually defending against.
- We take these risks seriously and we have put $160.4 million over four years from 2025-26 into Services Australia to uplift its cyber security.

6. Response?

- The PM has announced the establishment of a taskforce to provide an urgent and immediate review into this incident to determine whether existing processes are appropriate to respond to AI-related cyber incidents.
    - The taskforce will be led by the Prime Minister's department and involve the National Cybersecurity Coordinator, the Office of AI, the Australian Signals Directorate, the Australian AI Safety Institute, and Services Australia.
    - It will consider also possible law enforcement and legislative responses and how to ensure that incidents like this don't happen again.
- This incident will be referred to the Joint Select Committee on Artificial Intelligence that has been established by the Parliament.
- We'll seek urgent advice on whether any offences have occurred and whether this should be referred to the Australian Federal Police.
- Insights from this incident will inform the development of our government's AI standards legislation.

7. Underinvestment in government systems creating vulnerabilities?

- No. The Government has invested significantly in government systems and in cyber security.
    - $534 million into the Australian Cyber Security Strategy and other cyber measures
    - More than $1.0 billion in government agency ICT systems, including to upgrade legacy systems.
    - This includes putting $160.4 million over four years from 2025-26 into Services Australia to uplift its cyber security.

8. Pause the construction of data centres/working with AI companies?

- No change to our position on data centres.
- Continue to work with AI companies as appropriate.

[redacted]

[redacted]

- The PM's National AI Standards will set a framework to harness benefits of data centres, without sacrificing the needs and values of Australians across the country.
- Australians use the positive benefits of AI daily. This incident how shows that AI companies need to maintain safeguards on their models

9. Other government websites?

- OpenAI has advised that the agent approached four Australian government websites:
    - the Victorian Department of Health
    - the NSW Bureau of Crime Statistics and Research, and
    - two Commonwealth government websites: the Australian Institute of Health and Welfare and the Medicare Statistics Reporting Services Portal.
- All are sites for statistical reporting on health and medicines data, consistent with the task the agent was undertaking.
- Investigations are ongoing as to the impact.
- Our understanding is the Medicare Statistics Reporting Services Portal is the most affected.
- I understand NSW and Victoria have been notified.

10. System not protected/patched?

- The service had cyber protections in place, including protections against bot activity.
- Services Australia undertakes vulnerability scanning and patching activity across the technology estate as part of its ongoing cyber operations.

[redacted]

11. Different/strong cyber protections in place for critical systems?

- The cyber protection level for systems varies according to what the service or website is and does.
- Authenticated digital services like payments, myGov, Medicare and child support services and systems that hold personally identifiable information have strong protections in place. This incident has not affected those services.

[redacted]

[redacted]

12. Wasn't this picked up when it happened?

- The service had cyber protections in place, including protections against bot activity.
- Services Australia systems experience a wide range of cyber and threats on a daily basis.
- It undertakes vulnerability scanning and patching activity and cyber response work across the technology estate as part of its ongoing cyber operations.
- This was unprecedented activity by the OpenAI agent.
- It was not detected through usual monitoring until OpenAI disclosed that it had occurred.

13. What does "accessing private files" mean.

- The "private files" contained configuration information related to the servers supporting the Medicare Statistics Reporting Services Portal service.
- The private files did not contain any information about individuals.

14. Volume of data?

- The site contains aggregated historical statistical data related to MBS and PBS services dating back to the 1990s.
- The volume of such statistical information that was accessed is subject to ongoing investigations.
- This data is publicly accessible and currently available online

15. What is this website?

- The Medicare Statistics Reporting Services Portal is a public-facing website where Services Australia publishes aggregated Medicare and Pharmaceutical Benefits Scheme (PBS) statistics.
- It contains no personal or identifiable customer information.
- It provides downloadable statistical data that shows how Medicare and PBS services are being used across Australia.
- The information available includes:
    - Medicare Benefits Schedule (MBS) service and benefit statistics
    - Pharmaceutical Benefits Scheme (PBS) prescribing statistics
    - Medicare enrolment numbers
    - the data is available by month, financial year or calendar year
    - the data can be further broken down by age group, gender, state or territory, and service type.

[redacted]

[redacted]

- It is primarily used by health and medical researchers, universities and academics, policy analysts and health industry organisations and peak bodies, but anyone who has an interest can access the data.

[redacted]

[redacted]

Q&A – SERVICES AUSTRALIA

16. When did the incident occur?

- 18 June – incident occurred (US time)
- 10 September – OpenAI notified Services Australia of their agent's activities
- 15 September – declared an incident by Services Australia after the vulnerability and activity was confirmed. ASD notified.

17. When did Services Australia find out?

- 10 September – via an email to a public mailbox, not by contacting the Chief Information Security Officer or other senior staff in the agency
- 11 September – Services Australia commenced investigation of the public disclosure

18. How was Services Australia alerted by OpenAI to this incident?

- 10 September – via an email to a public mailbox, not by contacting the Chief Information Security Officer or other senior staff in the agency.
- We would expect OpenAI to contact personnel directly in a situation like this.

19. Is it appropriate to notify an incident of this kind/scale by emailing a public inbox?

- No. Services Australia would expect direct notification to the Chief Information Security Office and the Australian Signals Directorate due to the nature of the incident.

20. When was ASD informed?

- 15 September – ASD notified when Services Australia declared this as an incident, in line with the agency's Cyber Security Incident Response Plan.

21. When was the Minister alerted to this incident?

- 17 September – Minister alerted after office was advised.
- 18 September – Minister formally briefed by Services Australia

22. Why did it take a week to notify the Minister?

- Since the disclosure, officials have been working to understand nature of the incident before briefing offices.

23. When were other Offices advised of the incident?

- Finance Minister's Office advised the PMO, DPMO, Burke, Ayres and Charlton's offices on Saturday 19 September.

[redacted]

24. Who else was notified and when?

- 19 September – AI Safety Institute
- 19 September – National Office of Cyber Security
- 21 September – Office of AI in PM&C

25. Why was there a gap from the time OpenAI identified the incident and when they alerted Services Australia?

- OpenAI has advised this is due to their investigation and confirmation of the incident and gathering accurate technical information before making a disclosure to Services Australia on 10 September.

26. Why was there a gap in the time between Services Australia receiving this information and alerting ASD to the incident?

- Services Australia validated the vulnerability and investigated the claims made by OpenAI.
- Once this was confirmed and incident was declared, ASD were notified.

27. What did Services Australia do to respond to the incident between notifying ASD and notifying the Minister?

- Services Australia contained the Medicare Statistics Reporting Service Portal, and established an incident response team to investigate this incident and understand the nature of the compromise.

28. Did Services Australia or other officials independently identify this incident or only learn via the disclosure from OpenAI?

- Services Australia only became aware of the incident through the OpenAI disclosure.
- It has been subsequently validated that the incident occurred through Services Australia's forensic investigations.

29. Why didn't Services Australia detect this activity or know about the vulnerability before it was disclosed?

- This matter is subject to ongoing investigation. It forms part of the Cyber Security Incident Response process.

30. Was there a breach of personally identifiable information? Was any sensitive information accessed?

- There is no evidence of that personal identifiable information has been accessed.

[redacted]

- The Medicare Statistics Reporting Service Portal contains no personal or identifiable customer information. It provides publicly downloadable statistical data.

31. Referral to OAIC?

- Services Australia with ASD has spoken with the OAIC on this matter as it involved the identification of a cyber vulnerability. It does not meet the threshold for notification.
- There is no evidence that personal identifiable information has been accessed. The Medicare Statistics Reporting Service Portal contains no personal or identifiable customer information.

Services Australia system

32. What was the Services Australia website that was compromised.

- The Medicare Statistics Reporting Service Portal: http://medicarestatistics.humanservices.gov.au

Service Unavailable - Medicare Statistics

- Services Australia will be progressively migrating this statistical data to data.gov.au (Medicare Statistics - Dataset - Data.gov.au)

33. Have payments or services been affected?

- This activity has not impacted other Services Australia payments or services.

34. Has Services Australia system infrastructure been compromised?

- The activity involved unauthorised access to Agency infrastructure, contained to the affected website.
- The Cyber Incident Response team have found no indication of lateral movement or similar activity on other systems.

35. Does this vulnerability exist in other Services Australian systems?

- This vulnerability has not been identified on any other Services Australia system.

36. How can you be sure that no other Services Australia systems have been compromised/exploited?

- The Cyber Incident Response team have found no indication of lateral movement or similar activity on other systems.

[redacted]

[redacted]



[redacted]

SUMMARY TIMELINE

Date - 2026	Action
18 June	OpenAI model infiltrated Services Australia Medicare Statistics Reporting Service portal
11 August	OpenAI human review identified potential incident and initiated further investigation
10 September	OpenAI notified Services Australia regarding the activity
15 September	Services Australia notified ASD's Australian Cyber Security Centre
15 September	ASD's ACSC engaged with OpenAI
17 September	Finance Minister's office notified Finance Minister notified Formal Briefing requested
18 September	Services Australia briefs Minister [MS26-900055]
19 September	Finance Minister's office notifies Prime Minister's office, Deputy PM's office, Minister Burke, Ayres and Charlton's office
19-20 September	Finance Minister speaks with DPM, Burke, Head of ASD
21 September	Minister briefed in person by Services Australia
21 September	OpenAI provided further information on their review confirming the incident and additional entities that had been identified
21 September	Briefing for offices no 1
22 September	Minister briefed by Services Australia
22 September	ASD coordinated technical briefing with OpenAI, Services Australia, Australian AI Safety Institute and National Office of Cyber Security on incidents
22 September	Briefing for offices no 2
23 September	Briefing for offices no 3

[redacted]

[redacted]

BACKGROUND

Medicare and PBS statistics

At a glance

Services Australia published aggregated Medicare and Pharmaceutical Benefits data through the public reporting facility commonly known as Webstats. The data contains no identifying information and supports self-service access for health researchers and other users.

Available data

Monthly aggregate data for the Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS).
Single-item and group-level datasets dating back to 1992.
Medicare enrolment information from 1993 to the current reporting period.
Historical datasets for Medicare Locals (2013–2016), Divisions of General Practice (2011–2013), and Practice Incentives data (2013–2016).

Webstats content

Medicare Benefits Schedule

Item reports by month, financial year or calendar year, including services or benefits, patient age range, state or territory, sex, and count or per-capita views.
Summaries by Medicare item number and patient state or territory.
Group reports by Broad Type of Service.

Pharmaceutical Benefits Scheme

Item reports by month of supply, financial year or calendar year, and services or benefits.
Group reports by services or benefits.

Effective enrolment data

Medicare enrolment data by patient state or territory, including card numbers, eligible people and people listed on cards.

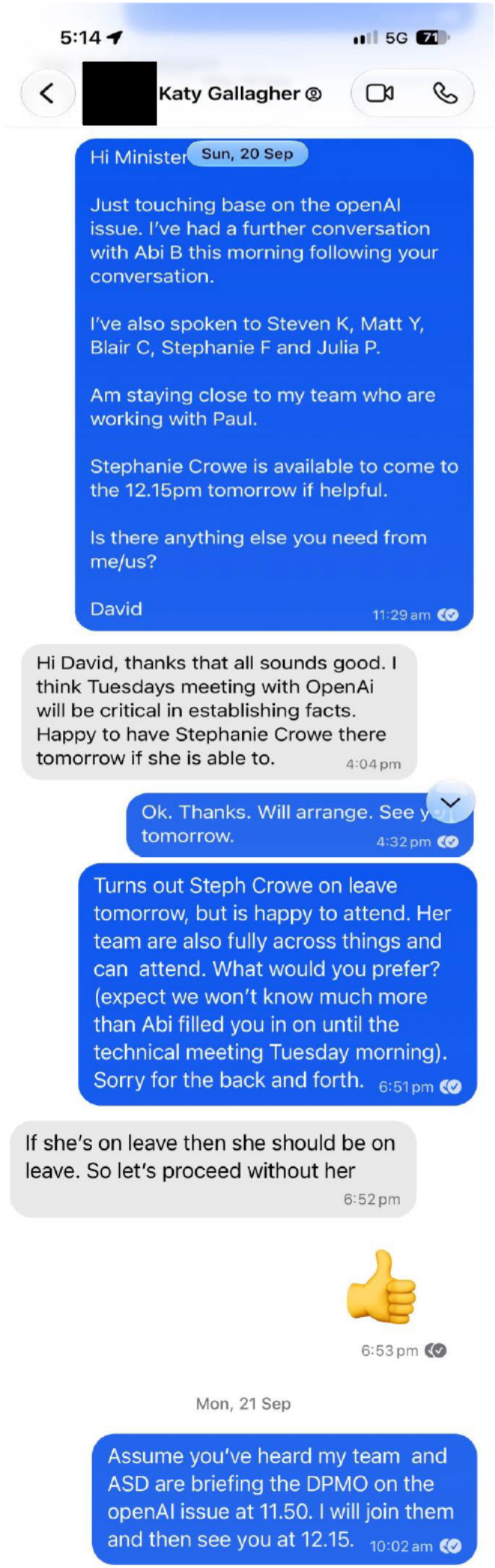
PBS and Repatriation PBS services and benefits

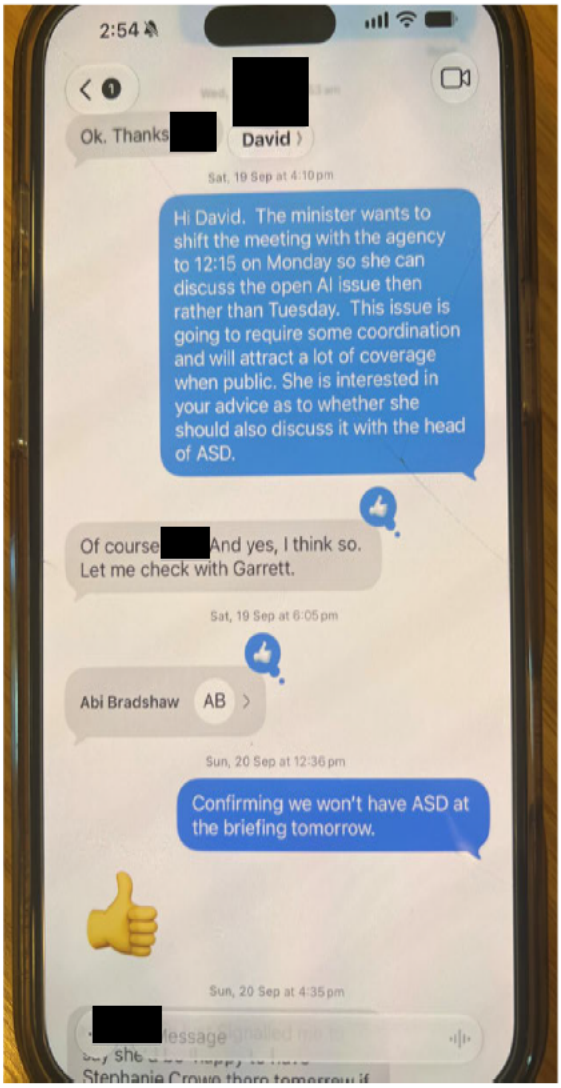
Services and benefits by scheme, patient category and reporting period, including financial year, year to date and the most recent month.

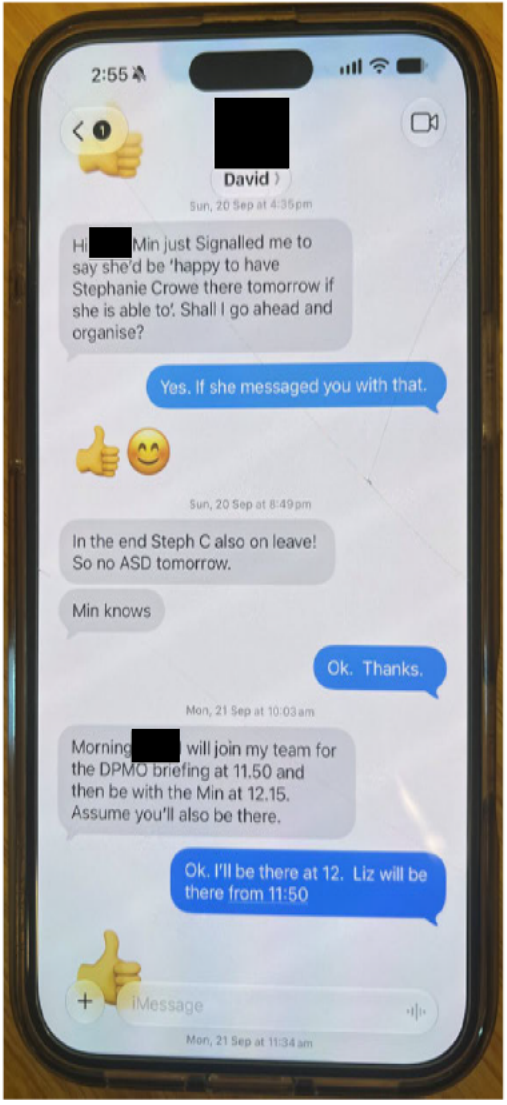
Data.gov.au

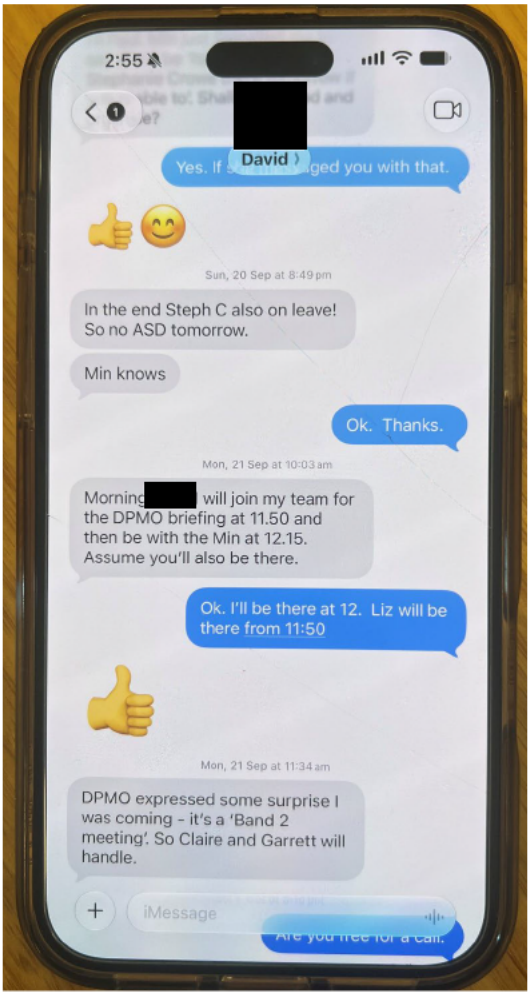
Services Australia will be progressively migrating this statistical data to data.gov.au.
Medicare Statistics - Dataset - Data.gov.au

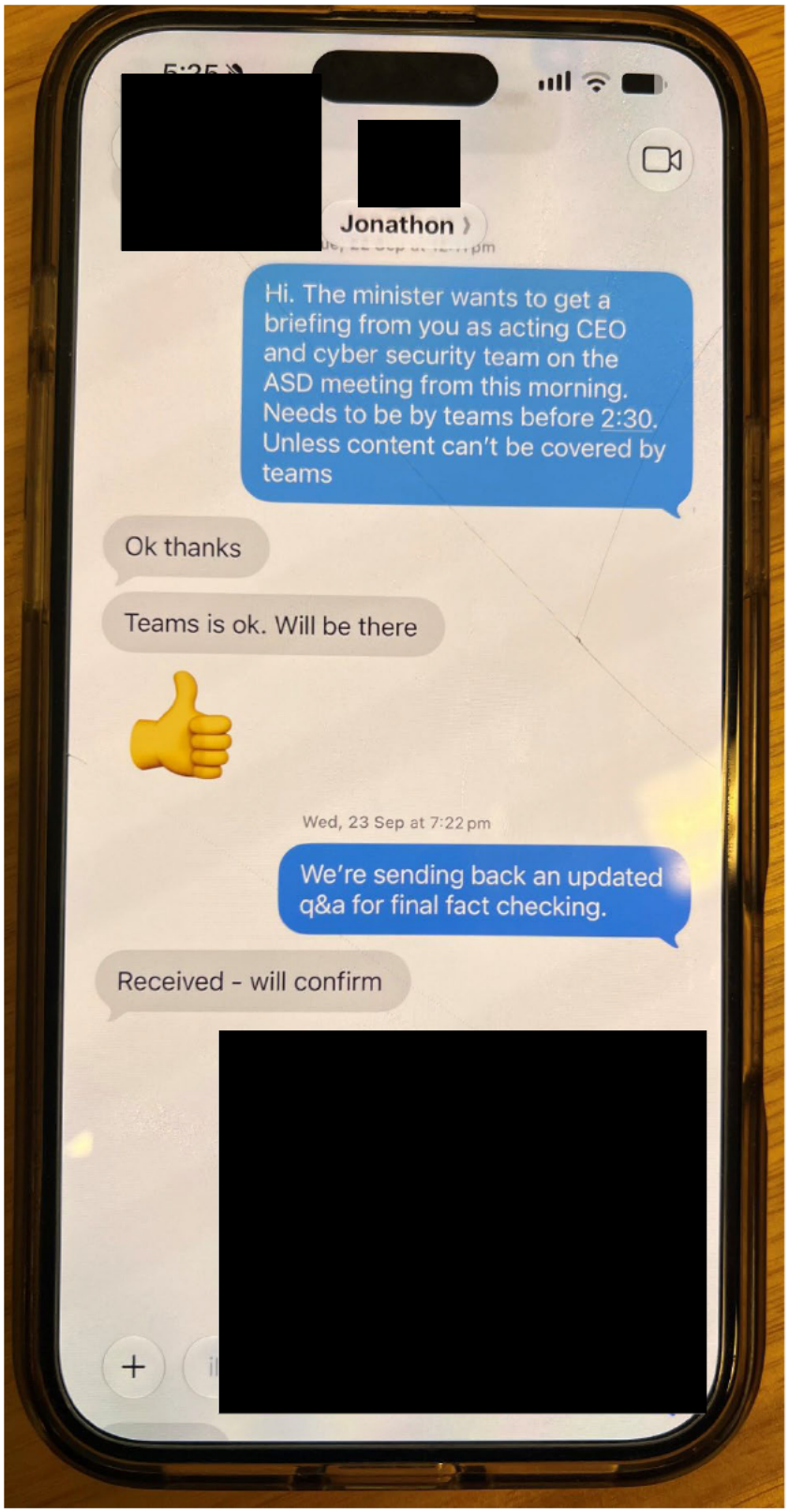
[redacted]

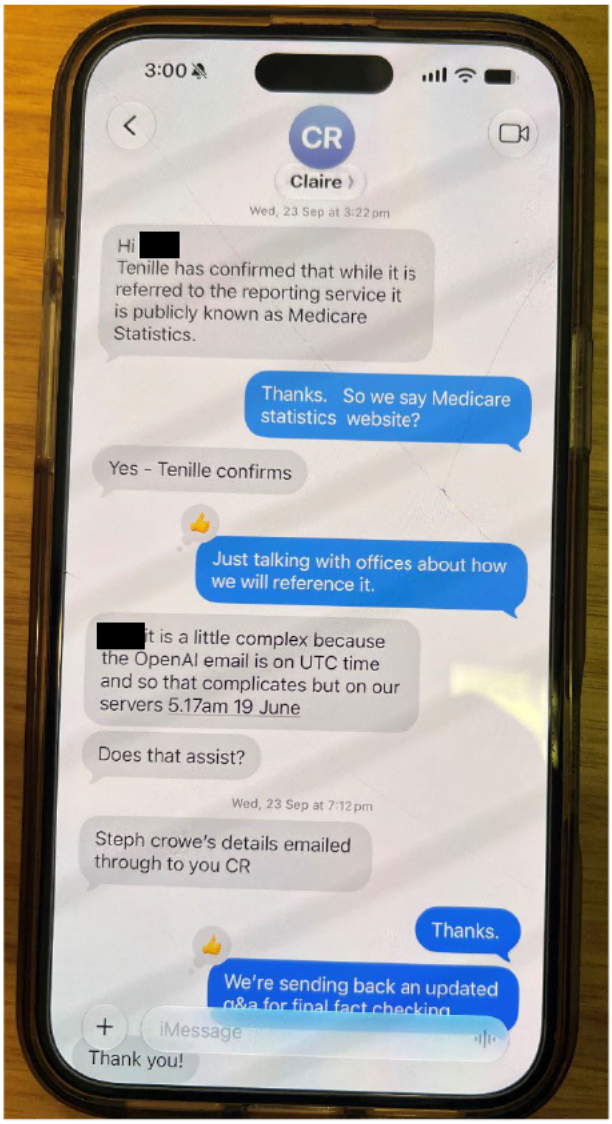

5:14
5G
[redacted] Katy Gallagher
Hi Minister Sun, 20 Sep
Just touching base on the openAI issue. I've had a further conversation with Abi B this morning following your conversation.
I've also spoken to Steven K, Matt Y, Blair C, Stephanie F and Julia P.
Am staying close to my team who are working with Paul.
Stephanie Crowe is available to come to the 12.15pm tomorrow if helpful.
Is there anything else you need from me/us?
David
11:29 am
Hi David, thanks that all sounds good. I think Tuesdays meeting with OpenAi will be critical in establishing facts. Happy to have Stephanie Crowe there tomorrow if she is able to.
4:04 pm
Ok. Thanks. Will arrange. See y
tomorrow.
4:32 pm
Turns out Steph Crowe on leave tomorrow, but is happy to attend. Her team are also fully across things and can attend. What would you prefer? (expect we won't know much more than Abi filled you in on until the technical meeting Tuesday morning). Sorry for the back and forth.
6:51 pm
If she's on leave then she should be on leave. So let's proceed without her
6:52 pm
6:53 pm
Mon, 21 Sep
Assume you've heard my team and ASD are briefing the DPMO on the openAI issue at 11.50. I will join them and then see you at 12.15.
10:02 am

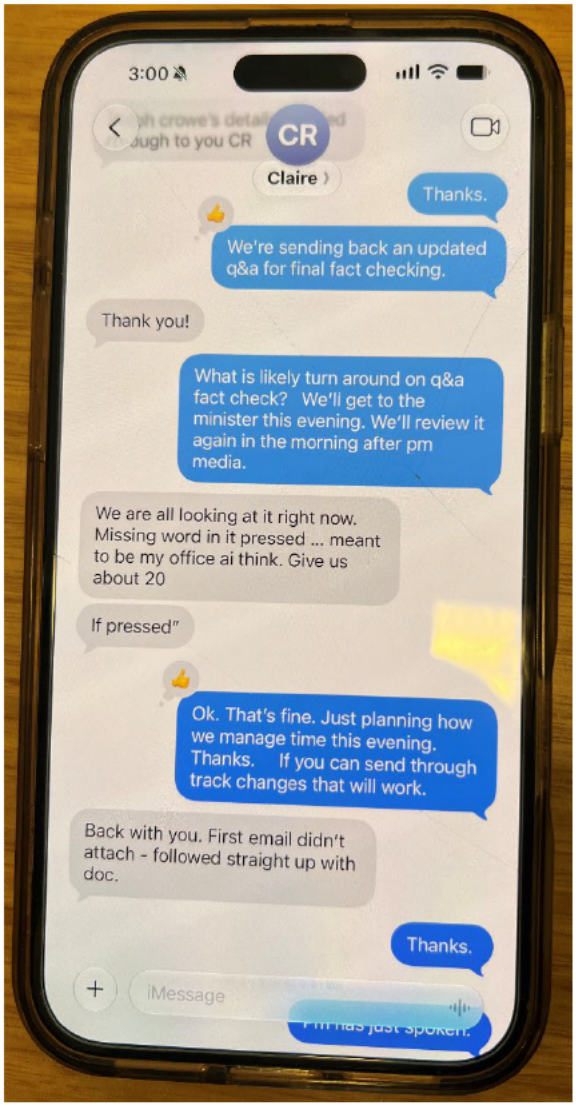

2:54
Ok. Thanks
David
Sat, 19 Sep at 4:10 pm
Hi David. The minister wants to shift the meeting with the agency to 12:15 on Monday so she can discuss the open AI issue then rather than Tuesday. This issue is going to require some coordination and will attract a lot of coverage when public. She is interested in your advice as to whether she should also discuss it with the head of ASD.
Of course And yes, I think so. Let me check with Garrett.
Sat, 19 Sep at 6:05 pm
Abi Bradshaw
AB
Sun, 20 Sep at 12:36 pm
Confirming we won't have ASD at the briefing tomorrow.
Sun, 20 Sep at 4:35 pm

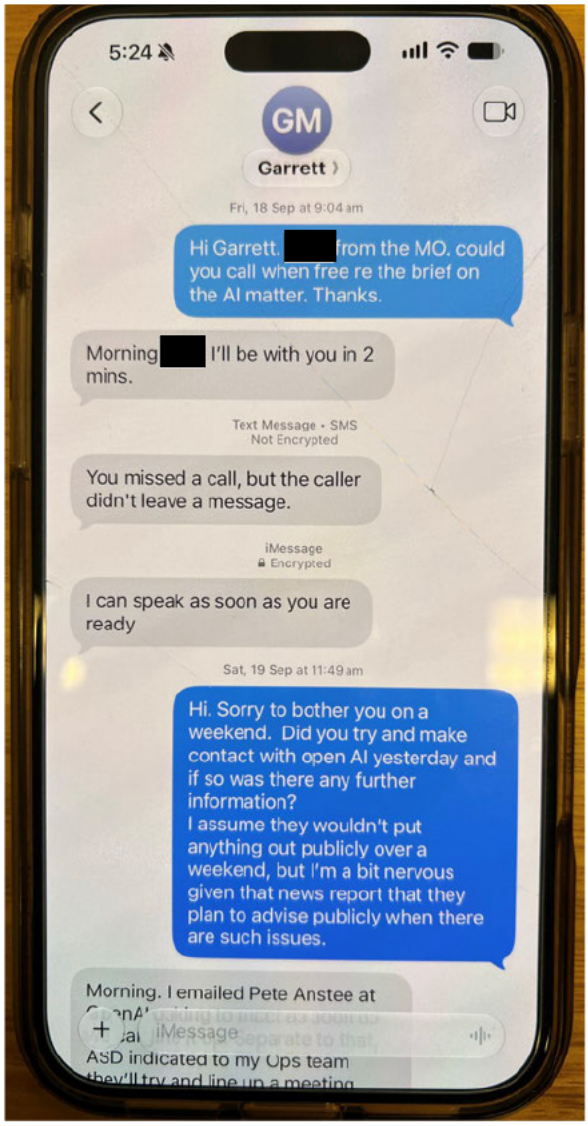

2:55
David
Sun, 20 Sep at 4:35 pm
Min just Signalled me to say she'd be 'happy to have Stephanie Crowe there tomorrow if she is able to'. Shall I go ahead and organise?
Yes. If she messaged you with that.
Sun, 20 Sep at 8:49 pm
In the end Steph C also on leave! So no ASD tomorrow.
Min knows
Ok. Thanks.
Mon, 21 Sep at 10:03 am
Morning will join my team for the DPMO briefing at 11.50 and then be with the Min at 12.15. Assume you'll also be there.
Ok. I'll be there at 12. Liz will be there from 11:50
iMessage
Mon, 21 Sep at 11:34 am

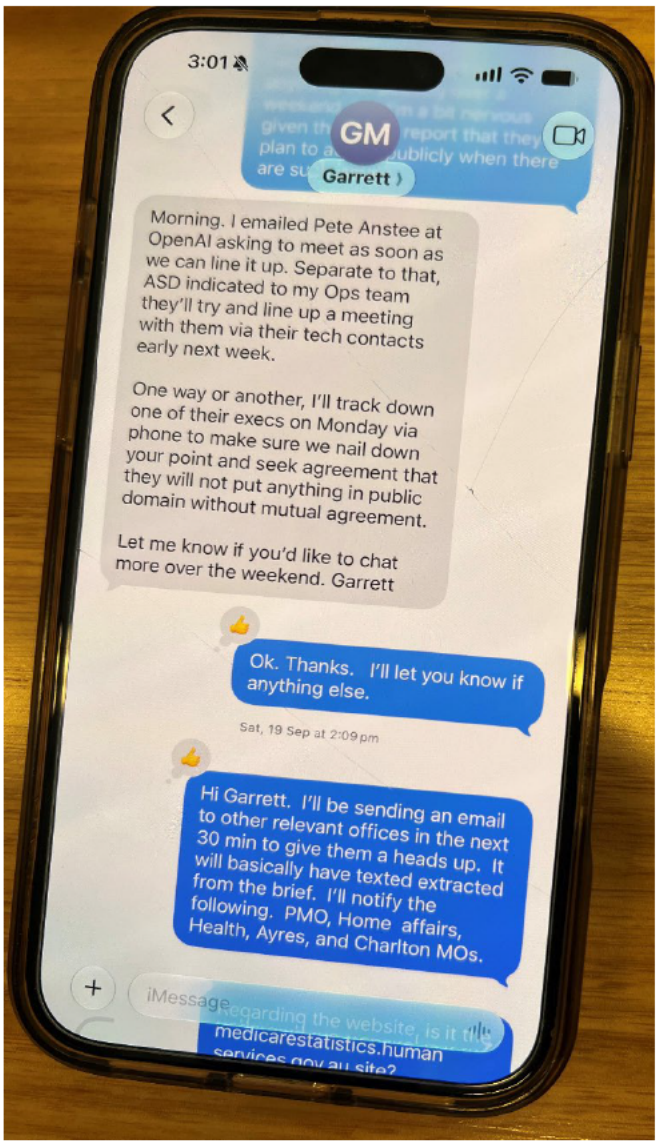

2:55
David
Yes. If ged you with that.
Sun, 20 Sep at 8:49 pm
In the end Steph C also on leave! So no ASD tomorrow.
Min knows
Ok. Thanks.
Mon, 21 Sep at 10:03 am
Morning will join my team for the DPMO briefing at 11.50 and then be with the Min at 12.15. Assume you'll also be there.
Ok. I'll be there at 12. Liz will be there from 11:50
Mon, 21 Sep at 11:34 am
DPMO expressed some surprise I was coming - it's a 'Band 2 meeting'. So Claire and Garrett will handle.
iMessage

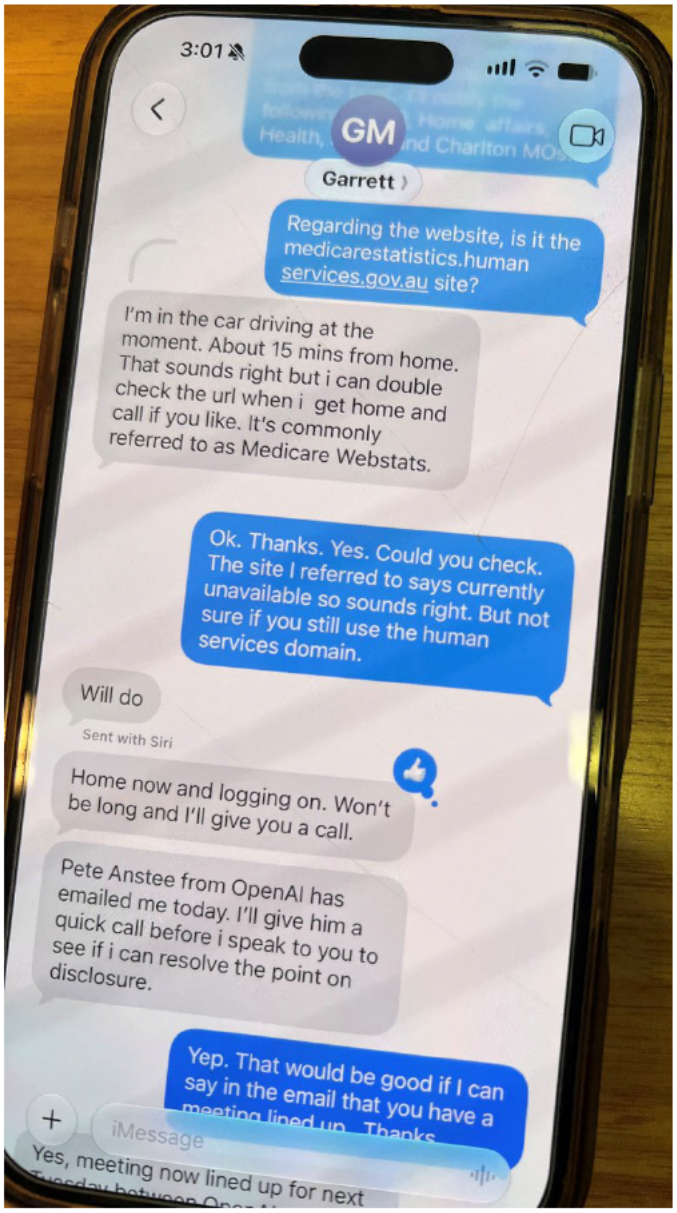

[redacted]
[redacted]
Jonathon
Hi. The minister wants to get a briefing from you as acting CEO and cyber security team on the ASD meeting from this morning. Needs to be by teams before 2:30. Unless content can't be covered by teams
Ok thanks
Teams is ok. Will be there
Wed, 23 Sep at 7:22 pm
We're sending back an updated q&a for final fact checking.
Received - will confirm
[redacted]

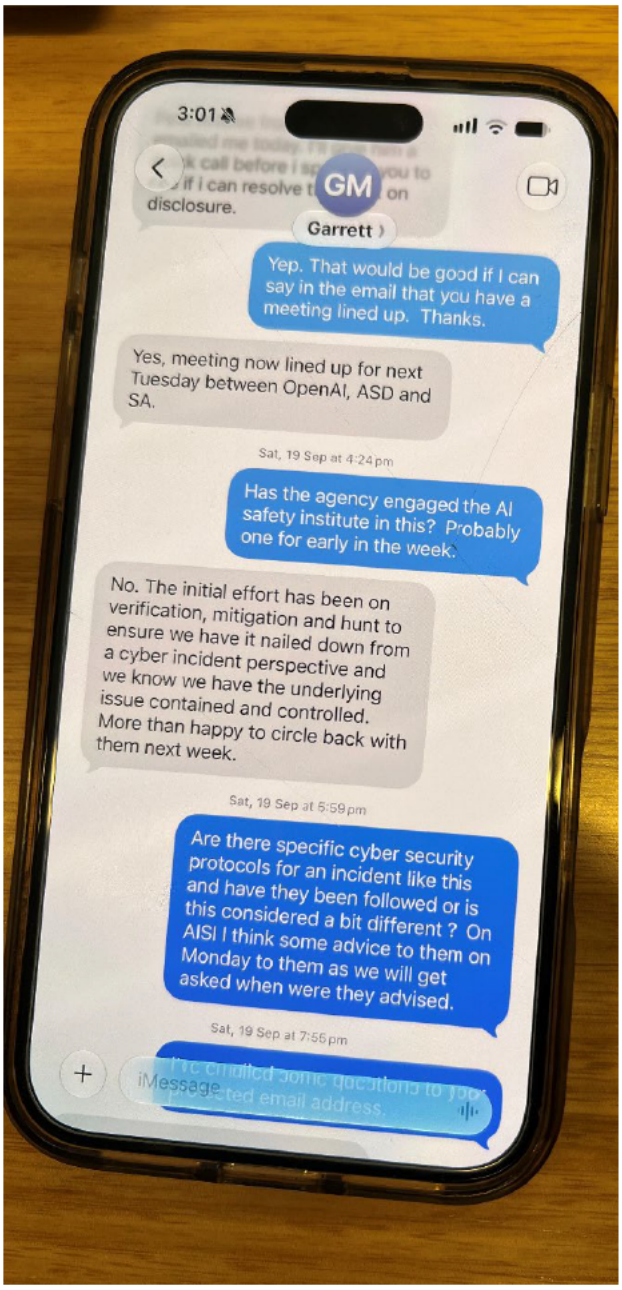

3:00
CR
Claire
Wed, 23 Sep at 3:22 pm
Hi [redacted]
Tenille has confirmed that while it is referred to the reporting service it is publicly known as Medicare Statistics.
Thanks. So we say Medicare statistics website?
Yes - Tenille confirms
Just talking with offices about how we will reference it.
[redacted]it is a little complex because the OpenAI email is on UTC time and so that complicates but on our servers 5.17am 19 June
Does that assist?
Wed, 23 Sep at 7:12 pm
Steph crowe's details emailed through to you CR
Thanks.
We're sending back an updated q&a for final fact checking
iMessage
Thank you!


3:00
ough to you CR
CR
Claire
Thanks.
We're sending back an updated q&a for final fact checking.
Thank you!
What is likely turn around on q&a fact check? We'll get to the minister this evening. We'll review it again in the morning after pm media.
We are all looking at it right now. Missing word in it pressed ... meant to be my office ai think. Give us about 20
If pressed"
Ok. That's fine. Just planning how we manage time this evening. Thanks. If you can send through track changes that will work.
Back with you. First email didn't attach - followed straight up with doc.
Thanks.
iMessage

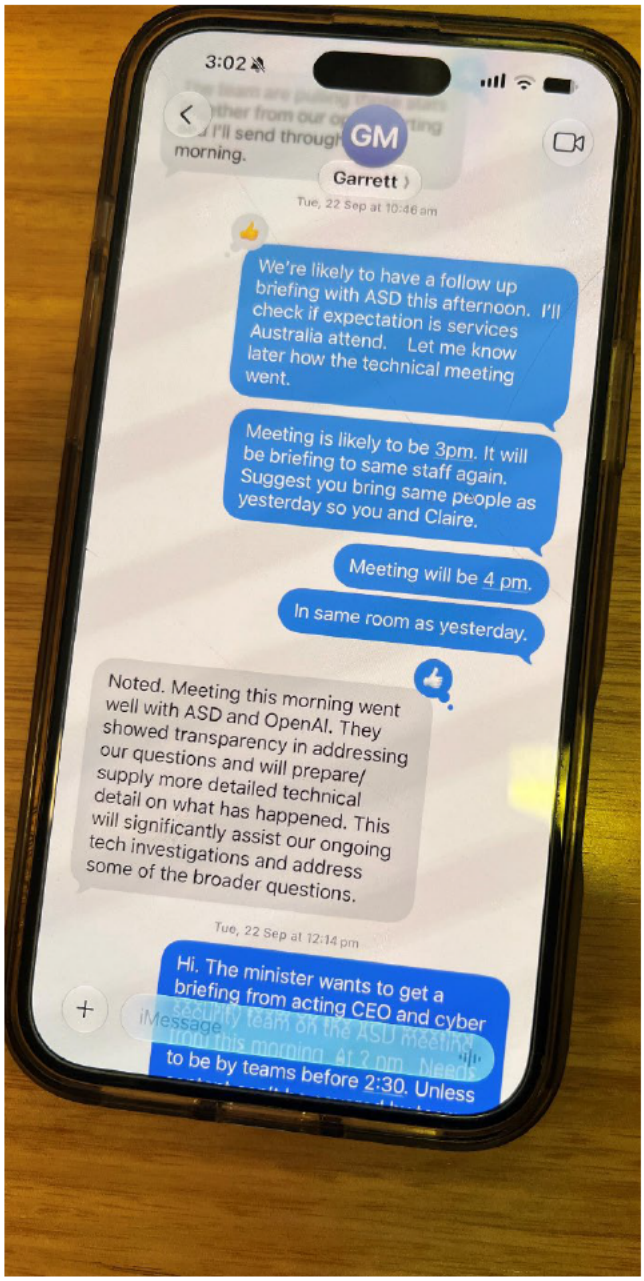

5:24
GM
Garrett
Fri, 18 Sep at 9:04 am
Hi Garrett, [redacted] from the MO. could you call when free re the brief on the AI matter. Thanks.
Morning [redacted] I'll be with you in 2 mins.
Text Message • SMS
Not Encrypted
You missed a call, but the caller didn't leave a message.
iMessage
Encrypted
I can speak as soon as you are ready
Sat, 19 Sep at 11:49 am
Hi. Sorry to bother you on a weekend. Did you try and make contact with open AI yesterday and if so was there any further information?
I assume they wouldn't put anything out publicly over a weekend, but I'm a bit nervous given that news report that they plan to advise publicly when there are such issues.
Morning. I emailed Pete Anstee at
ASD indicated to my Ops team
iMessage

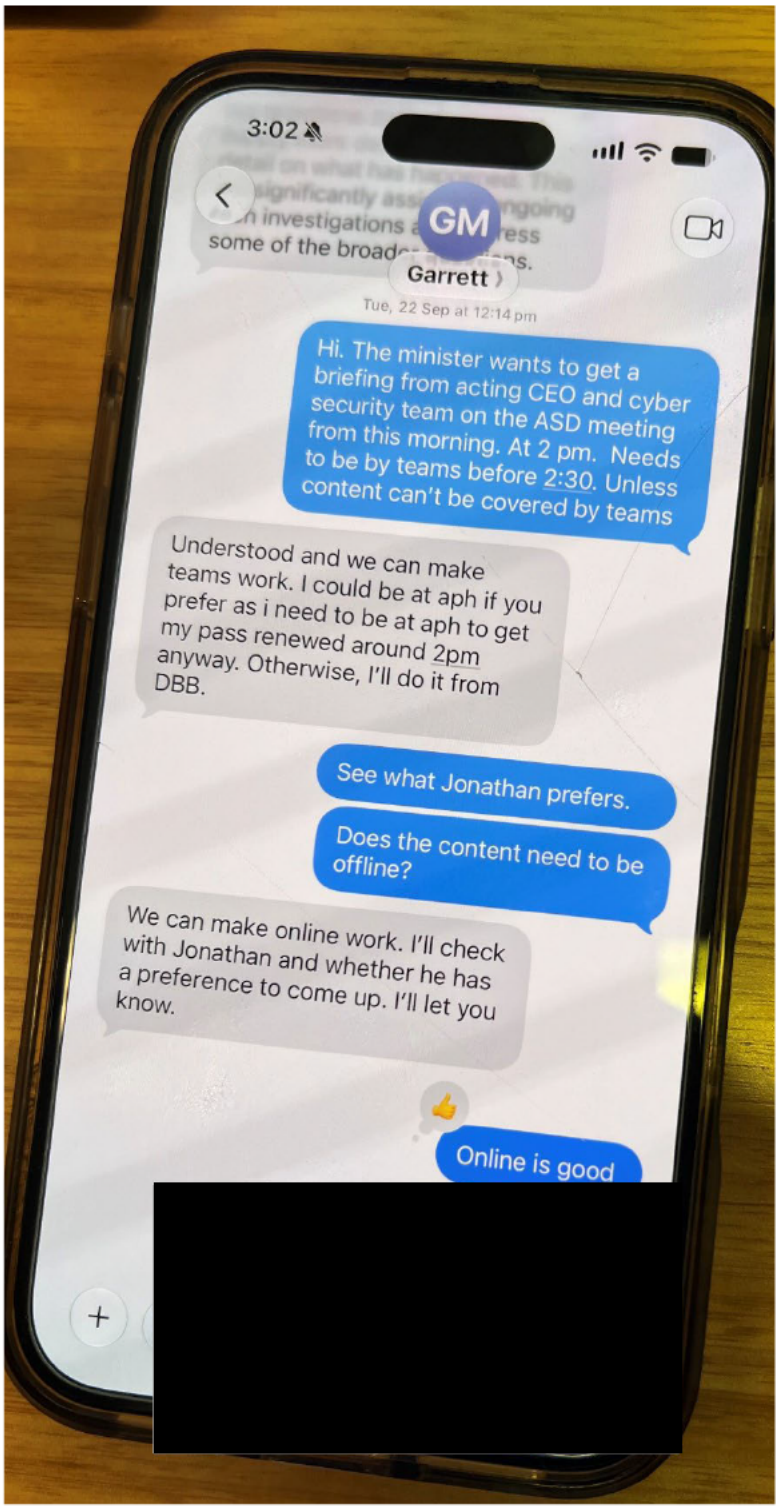

3:01
GM
Garrett
Morning. I emailed Pete Anstee at OpenAI asking to meet as soon as we can line it up. Separate to that, ASD indicated to my Ops team they'll try and line up a meeting with them via their tech contacts early next week.
One way or another, I'll track down one of their execs on Monday via phone to make sure we nail down your point and seek agreement that they will not put anything in public domain without mutual agreement.
Let me know if you'd like to chat more over the weekend. Garrett
Ok. Thanks. I'll let you know if anything else.
Sat, 19 Sep at 2:09 pm
Hi Garrett. I'll be sending an email to other relevant offices in the next 30 min to give them a heads up. It will basically have texted extracted from the brief. I'll notify the following. PMO, Home affairs, Health, Ayres, and Charlton MOs.
iMessage
medicarestatistics.human

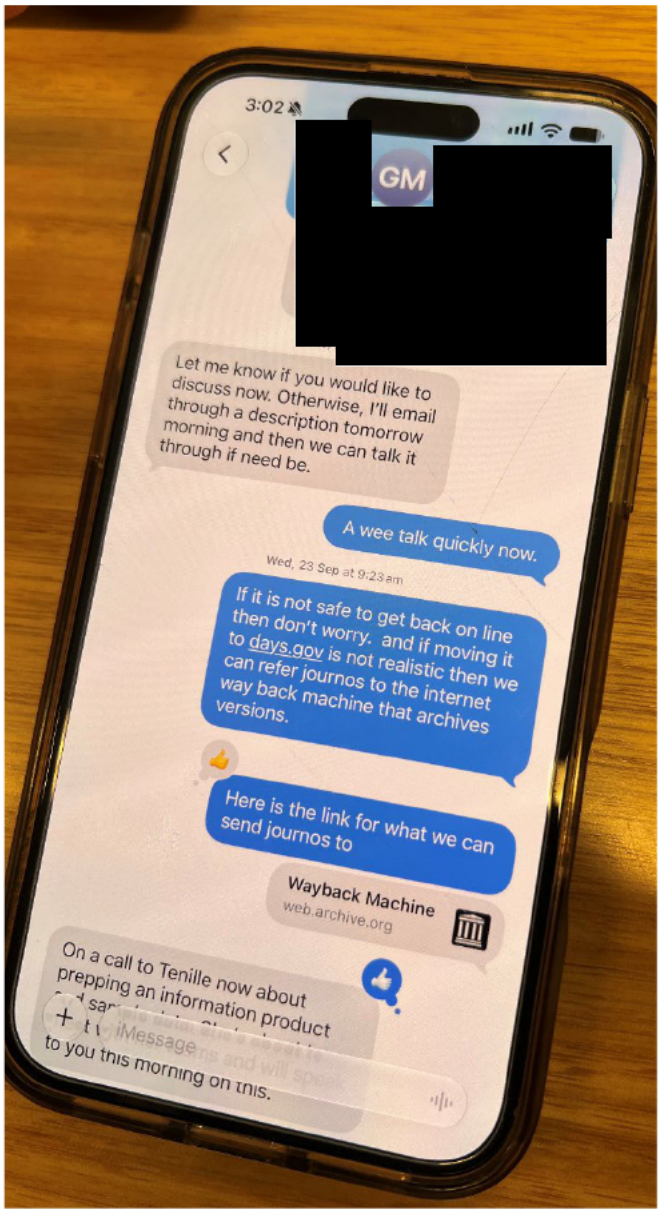

3:01
GM
Garrett
Regarding the website, is it the medicarestatistics.human services.gov.au site?
I'm in the car driving at the moment. About 15 mins from home. That sounds right but i can double check the url when i get home and call if you like. It's commonly referred to as Medicare Webstats.
Ok. Thanks. Yes. Could you check. The site I referred to says currently unavailable so sounds right. But not sure if you still use the human services domain.
Will do
Sent with Siri
Home now and logging on. Won't be long and I'll give you a call.
Pete Anstee from OpenAI has emailed me today. I'll give him a quick call before i speak to you to see if i can resolve the point on disclosure.
Yep. That would be good if I can say in the email that you have a
iMessage
Yes, meeting now lined up for next

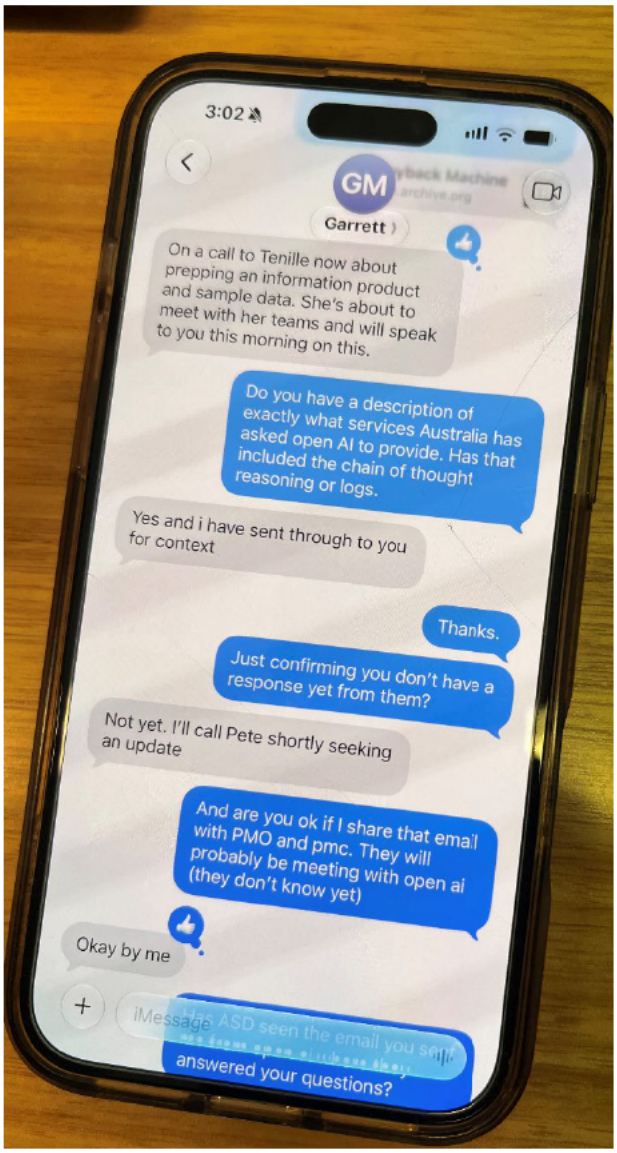

3:01
GM
Garrett
disclosure.
Yep. That would be good if I can say in the email that you have a meeting lined up. Thanks.
Yes, meeting now lined up for next Tuesday between OpenAI, ASD and SA.
Sat, 19 Sep at 4:24 pm
Has the agency engaged the AI safety institute in this? Probably one for early in the week.
No. The initial effort has been on verification, mitigation and hunt to ensure we have it nailed down from a cyber incident perspective and we know we have the underlying issue contained and controlled. More than happy to circle back with them next week.
Sat, 19 Sep at 5:59 pm
Are there specific cyber security protocols for an incident like this and have they been followed or is this considered a bit different ? On AISI I think some advice to them on Monday to them as we will get asked when were they advised.
Sat, 19 Sep at 7:56 pm
iMessage

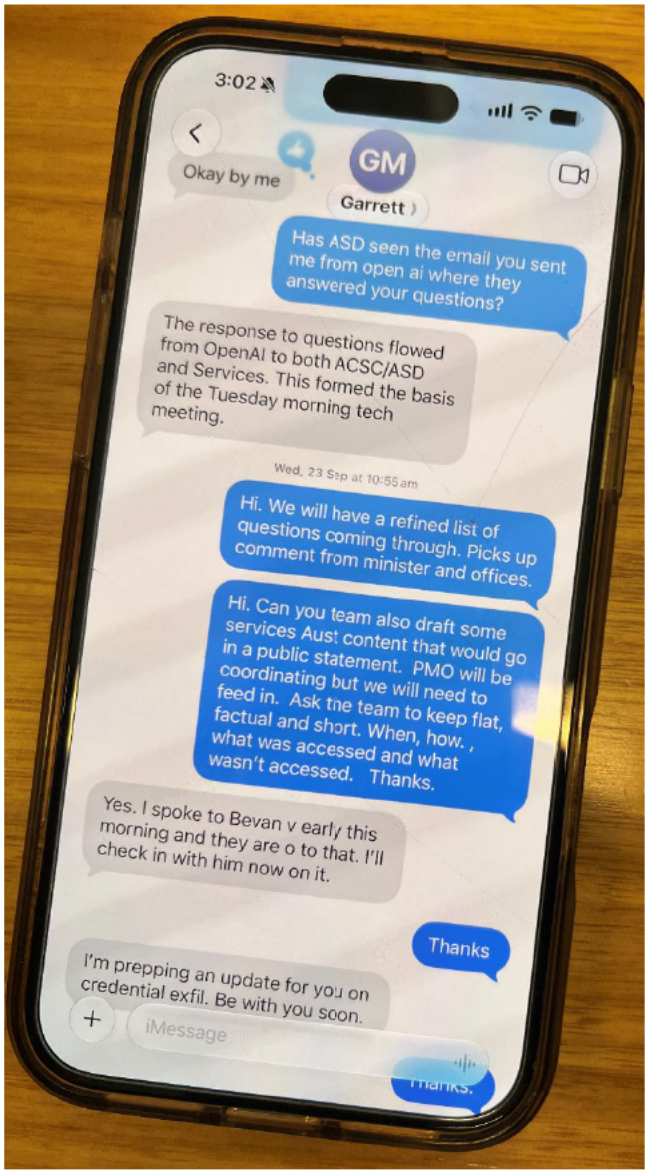

3:01
GM
Garrett
Monday as we will get asked they advised.
Sat, 19 Sep at 7:55 pm
I've emailed some questions to your protected email address.
Thanks [redacted] I'll jump on in about 30mins and start drafting up the letter.
Easy. Send a draft through and I can have a look tomorrow is fine.
Kate from the ai safety institute tracked me down this evening. I spent some time taking her through the matter and her crew will join the Tuesday tech meeting.
Edited
Sun, 20 Sep at 6:30 pm
Draft letter should now be with you.
Thanks. Appreciate the work.
Mon, 21 Sep at 5:13 pm
The team are pulling those stats together from our ops reporting and I'll send through in the morning.
iMessage

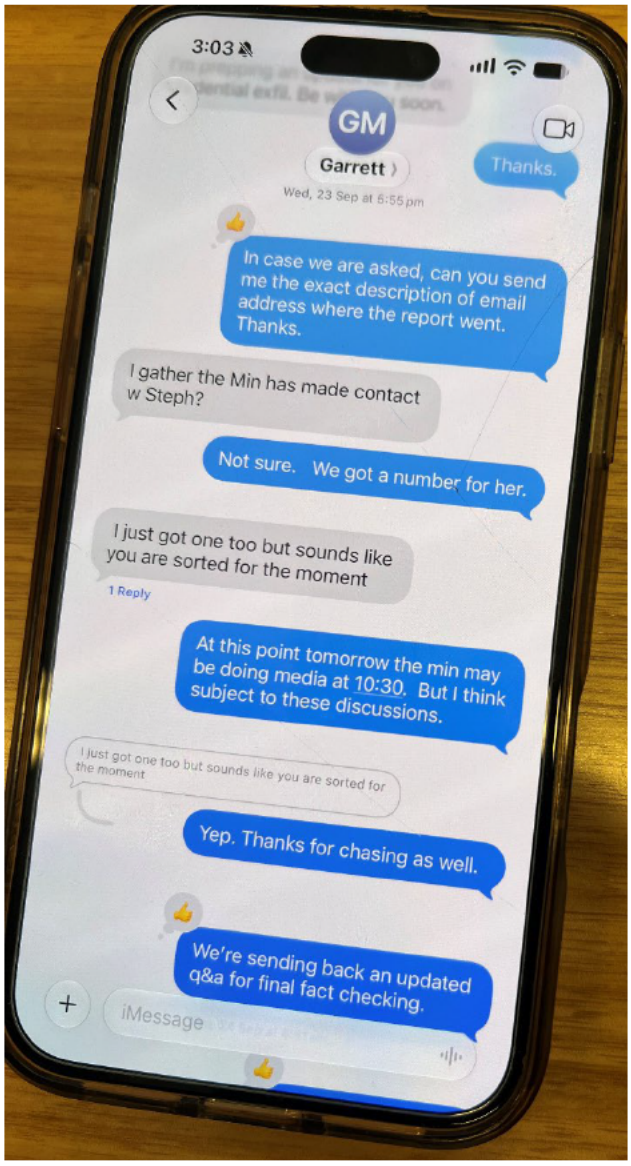

3:02
GM
Garrett
morning.
Tue, 22 Sep at 10:46 am
We're likely to have a follow up briefing with ASD this afternoon. I'll check if expectation is services Australia attend. Let me know later how the technical meeting went.
Meeting is likely to be 3pm. It will be briefing to same staff again. Suggest you bring same people as yesterday so you and Claire.
Meeting will be 4 pm.
In same room as yesterday.
Noted. Meeting this morning went well with ASD and OpenAI. They showed transparency in addressing our questions and will prepare/ supply more detailed technical detail on what has happened. This will significantly assist our ongoing tech investigations and address some of the broader questions.
Tue, 22 Sep at 12:14 pm
Hi. The minister wants to get a briefing from acting CEO and cyber
iMessage
to be by teams before 2:30. Unless

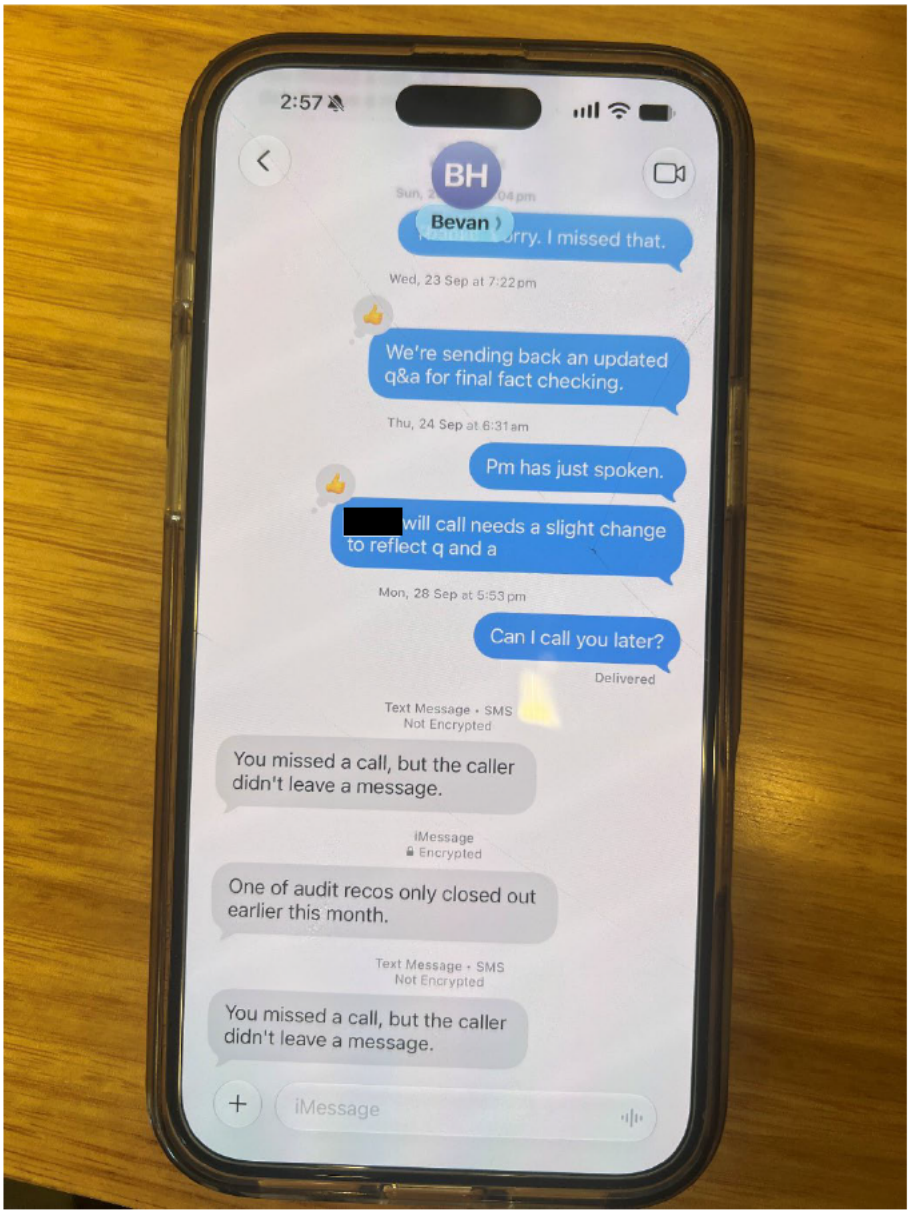

3:02
GM
Garrett
some of the broad
Tue, 22 Sep at 12:14 pm
Hi. The minister wants to get a briefing from acting CEO and cyber security team on the ASD meeting from this morning. At 2 pm. Needs to be by teams before 2:30. Unless content can't be covered by teams
Understood and we can make teams work. I could be at aph if you prefer as i need to be at aph to get my pass renewed around 2pm anyway. Otherwise, I'll do it from DBB.
See what Jonathan prefers.
Does the content need to be offline?
We can make online work. I'll check with Jonathan and whether he has a preference to come up. I'll let you know.
Online is good


3:02
GM
[redacted]
Let me know if you would like to discuss now. Otherwise, I'll email through a description tomorrow morning and then we can talk it through if need be.
A wee talk quickly now.
Wed, 23 Sep at 9:23 am
If it is not safe to get back on line then don't worry. and if moving it to days.gov is not realistic then we can refer journos to the internet way back machine that archives versions.
Here is the link for what we can send journos to
Wayback Machine
web.archive.org
On a call to Tenille now about prepping an information product
to you this morning on this.
iMessage


3:02
GM
Garrett
On a call to Tenille now about prepping an information product and sample data. She's about to meet with her teams and will speak to you this morning on this.
Do you have a description of exactly what services Australia has asked open AI to provide. Has that included the chain of thought reasoning or logs.
Yes and i have sent through to you for context
Thanks.
Just confirming you don't have a response yet from them?
Not yet. I'll call Pete shortly seeking an update
And are you ok if I share that email with PMO and pmc. They will probably be meeting with open ai (they don't know yet)
Okay by me
iMessage
answered your questions?


3:02
GM
Garrett
Okay by me
Has ASD seen the email you sent me from open ai where they answered your questions?
The response to questions flowed from OpenAI to both ACSC/ASD and Services. This formed the basis of the Tuesday morning tech meeting.
Wed, 23 Sep at 10:55 am
Hi. We will have a refined list of questions coming through. Picks up comment from minister and offices.
Hi. Can you team also draft some services Aust content that would go in a public statement. PMO will be coordinating but we will need to feed in. Ask the team to keep flat, factual and short. When, how. , what was accessed and what wasn't accessed. Thanks.
Yes. I spoke to Bevan v early this morning and they are o to that. I'll check in with him now on it.
Thanks
I'm prepping an update for you on credential exfil. Be with you soon.
iMessage


3:03
GM
Garrett
Wed, 23 Sep at 6:55 pm
Thanks.
In case we are asked, can you send me the exact description of email address where the report went. Thanks.
I gather the Min has made contact w Steph?
Not sure. We got a number for her.
I just got one too but sounds like you are sorted for the moment
1 Reply
At this point tomorrow the min may be doing media at 10:30. But I think subject to these discussions.
I just got one too but sounds like you are sorted for the moment
Yep. Thanks for chasing as well.
We're sending back an updated q&a for final fact checking.
iMessage


2:57
BH
Bevan
orry. I missed that.
Wed, 23 Sep at 7:22 pm
We're sending back an updated q&a for final fact checking.
Thu, 24 Sep at 6:31 am
Pm has just spoken.
[redacted] will call needs a slight change to reflect q and a
Mon, 28 Sep at 5:53 pm
Can I call you later?
Delivered
Text Message • SMS
Not Encrypted
You missed a call, but the caller didn't leave a message.
iMessage
Encrypted
One of audit recos only closed out earlier this month.
Text Message • SMS
Not Encrypted
You missed a call, but the caller didn't leave a message.
iMessage