# The Outside Report Test

*When someone outside your company finds a problem in your systems, how long until the right person knows? One test email tells you.*

On June 18, an internal OpenAI agent reached an Australian Medicare statistics portal. Australia didn't hear about it until OpenAI emailed a government inbox on September 10, nearly three months later. Government Services Minister Katy Gallagher said that inbox was checked once a day.

This sheet times the path from an outside report to the person who can act on it.

## Walk the path

Answer each one for your company. A blank means the report stops there.

| QUESTION | OUR ANSWER | WHO OWNS IT |
|---|---|---|
| Where does an outsider send a report? | | |
| Does it promise no legal action against good-faith reporters? | | |
| Who reads it, and how often? | | |
| Who can they reach at 2 a.m.? | | |
| How do they find the owner of an old system? | | |
| Who decides what we tell customers and regulators? | | |

## Time it

From a personal email, send a report to the address you published. Name one real system and write: "TEST. Treat this as a live report and route it to this system's owner. Don't touch the system." Tell one executive first, and nobody on the path you're testing.

**Sent at** _____ **First reply from a person** _____

**System owner knew** _____ **Hours from report to owner** _____

PASS OR FAIL

**Pass: the system's owner knew within four hours, whatever day and time you sent it. Fail: anything slower, an auto-reply, or no answer. A mailbox checked once a day can't pass.**

The four hours is my suggestion, not a standard. If you failed, fix the inbox before anything else on this page.

## Check what an outsider can reach

Two related cases from the same round of testing, separate from Medicare, point at what else to check.

- [ ] Pre-production and test servers closed to the outside. The research group Transluce found that when OpenAI's agents were blocked on the main site of the Australian Institute of Health and Welfare, they fetched the same file, which was public, from its pre-production server.
- [ ] Leaked keys and passwords revoked, with access logs checked for use. OpenAI says its agents found an exposed access key at the Victorian Agency for Health Information.
- [ ] Every old system still reachable from the internet has a named owner. The Medicare portal was a legacy system, and it has since been shut down.

## Decide this week

**Our published contact for reports** _____ **Who reads it (a name)** _____

**Our oldest system facing the internet** _____ **Its owner (a name)** _____

**Date we send the next test report** _____

**What this sheet is and is not.** As of September 29, 2026, neither OpenAI nor the Australian government had published how the agent got past the portal's controls. The Medicare and inbox details come from ABC News, SBS and TechCrunch reporting from September 24 to 29, 2026. The pre-production case is from Transluce's report of September 23, and the access key from OpenAI's own account and iTnews. If your business has a legal reporting deadline, that one wins.

*I sell AI software, and this story is about an AI agent reaching somewhere it shouldn't. You don't need anything from me to send a test email.*

**Scan for more field kits**

Every worksheet and every issue of Enterprise Field Notes, free at benpickett.com

Ben Pickett

© 2026 Enterprise Field Notes