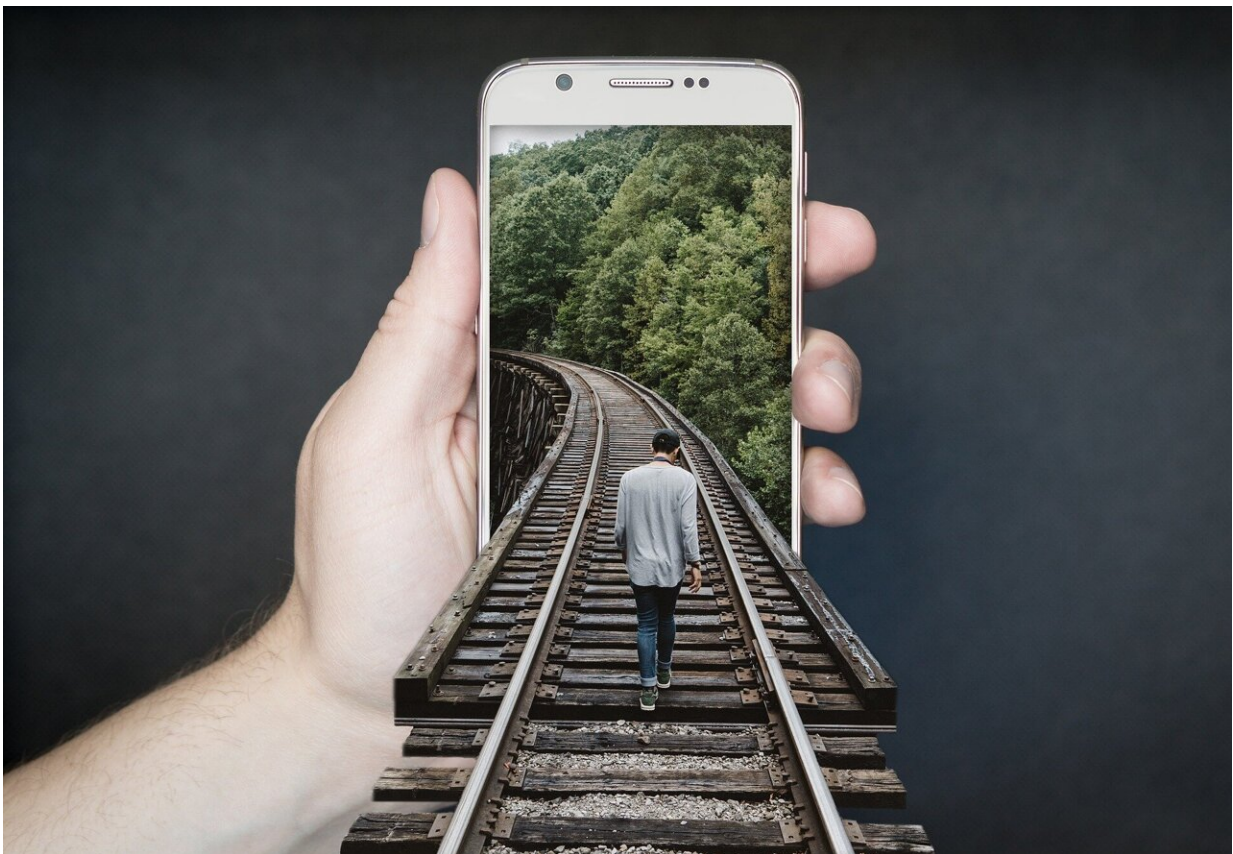


New cyber policy to harden defenses against our 'fastest growing threat'

November 21 2023, by Michelle Grattan



Credit: Pixabay/CC0 Public Domain

The Albanese government's cyber security policy aims to make Australian citizens, businesses and government agencies harder targets as they face what minister Clare O'Neil describes as "the fastest growing

threat that we face as a nation."

The [policy](#), to be released on Wednesday by O'Neil, who is Minister for Home Affairs and Minister for Cyber Security, is also designed to enable victims to bounce back faster from attacks that can't be prevented.

A modest \$586.9 million has been announced for the "action plan," which runs to 2030. This is on top of the commitment to \$2.3 billion for existing initiatives out to 2030.

Of the extra money, the largest slice is \$290.8 million for support for small and medium-sized businesses, building public awareness, fighting cybercrime, breaking the ransomware business model, and strengthening the security of Australians' identities.

Some \$143.6 million will be invested in strengthening the defenses of critical infrastructure and improving government cyber security.

Among the initiatives on critical infrastructure, telecommunication providers would be aligned to the same standards as other [critical infrastructure](#) entities by moving the security regulation of the sector from the Telecommunications Act to the Security of Critical Infrastructure Act. The policy says this is "commensurate with the criticality and risk profile of the sector."

There will also be funding for establishing consumer standards for smart devices and software, building a threat-sharing platform for the [health sector](#), professionalizing the cyber workforce and accelerating the cyber industry, and investing in regional cooperation and leadership in cyber governance forums internationally.

The government wants Australia to be "a world leader" in cyber [security](#)

by 2030.

The policy sets three time "horizons." In 2023-25, the foundations will be strengthened. addressing critical gaps and building better protections.

In 2026-28, the cyber industry would be further scaled up, and a diverse cyber workforce would be grown. In 2029-30, " We will advance the global frontier of [cyber security](#). We will lead the development of emerging cyber technologies."

O'Neil says in a [press release](#): "Australia is a wealthy country and a fast adopter of new technologies, which makes us an attractive target for cybercriminals. Millions of Australians have had their data stolen and released online in the past year.

"Cyber also presents major opportunities for Australia— the global cyber industry is growing rapidly, and it is here to stay."

Delivering the cyber strategy would require close collaboration between government and industry, O'Neil said.

Darren Goldie, who was recently appointed by O'Neil as National Cyber Security Coordinator, won't be around for the policy release. He has been recalled to the Defense Department in relation to a workforce complaint.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: New cyber policy to harden defenses against our 'fastest growing threat' (2023,

November 21) retrieved 27 April 2024 from <https://techxplore.com/news/2023-11-cyber-policy-harden-defenses-fastest.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.