Australian Government

Australian Government response to the Parliamentary Joint Committee on Law Enforcement report:

Impact of New and Emerging Information and Communication Technology

NOVEMBER 2025

Recommendations made in Impact of new and emerging information and communication technology

Committee Recommendations

Recommendation 1:

The committee recommends that the National Cybercrime Working Group examines and reports on the merits of the following initiatives as part of its work developing a new National Plan to Combat Cybercrime:

- a national statutory framework for Delayed Notification Search Warrants for serious crime and corruption offences;
- a framework for an Indicators and Warning system, to sit within the ACIC, aimed at identifying disruptive changes in the global illicit supply chains that impact on Australia's market;
- an independent entity to review current case categorisation and prioritisation models used by agencies within the Home Affairs Portfolio; and
- a review of how existing law enforcement strategies to tackle activities facilitated by the dark web, such as that used to close Silk Road, can be enhanced for wider application.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 2:

The committee recommends that the Australian government considers establishing a task force comprising information and communications technology (ICT), legal, law enforcement and security experts, including from academia, to:

- monitor the development, and examine and advise on the impact of new and emerging ICTs on Australian law enforcement;
- identify specific gaps and vulnerabilities in the current legislative and regulatory frameworks that may be limiting the ability of Australian law enforcement agencies to investigate, disrupt or otherwise deal with cybercrime, including encryption services and encrypted devices;
- consult and advise on the balance between investigatory powers to tackle cybercrime and their impact on civil rights and liberties;
- report to the Australian government at regular intervals on the appropriateness of current legislative and regulatory frameworks; and
- recommend any changes that may be necessary to ensure that law enforcement agencies are keeping pace with and capable of tackling new cyber challenges as they arise.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 3:

The committee recommends that the Australian government evaluates the current *Mutual Legal Assistance Treaty* process and identifies:

- how the process might be modified to better suit the investigation of cybercrimes and the information and communications technology challenges facing law enforcement; and
- opportunities to implement those modifications with treaty partners.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 4:

The committee recommends that the Australian government explores a range of approaches for improving the information and communications technology (ICT) skills and capabilities of the law enforcement workforce, including:

- engaging volunteer experts, similar to the United Kingdom (UK) National Crime Agency Specials program;
- establishing 'single points of contact' within law enforcement agencies, similar to the approach adopted in the UK;
- implementing a single Commonwealth-led cooperative entity, providing expert cybercrime investigative support services to government, national security and law enforcement agencies; and
- establishing ICT cadetship programs for the recruitment of talented university students.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 5:

The committee recommends that the Australian government explores suggestions from law enforcement agencies and cybersecurity experts for improving information and communications technology (ICT) capabilities and resources, including:

- dedicated agency funding with sufficient flexibility to enable law enforcement agencies to respond to the escalating challenges of cybercrime; and
- improving the model of ICT procurement and project management to promote new and emerging ICT for operational purposes.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 6:

The committee recommends the Australian government considers the use of hybrid storage strategies, artificial intelligence and other advanced techniques for sorting, filtering and analysing large volumes of data.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 7:

The committee recommends that the Australian government takes the following into account when developing any future strategies for biometric data and facial recognition systems:

- the development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security;
- the use of methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities; and
- publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 8:

The committee recommends that the Australian government reviews current consumer protection laws and regulations in relation to internet-enabled devices and identifies changes that may be required to provide adequate and timely consumer protection in relation to the risks they pose.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 9:

The committee recommends that Australian governments review legal mechanisms intended to protect victims, such as *Apprehended Violence Orders*, to ensure that they offer adequate protection to victims of crime facilitated by internet-enabled devices.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 10:

The committee recommends that the Australian government develops education materials to inform law enforcement agencies and personnel about new and emerging information and communications technologies that offenders may use to facilitate family and domestic abuse, and to provide guidance on appropriate strategies for responding to such situations.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 11:

The committee recommends that the Australian government develops and implements an Internet of Things (IoT) public awareness campaign that:

- raises awareness about the potential vulnerabilities of internet-enabled devices and the IoT; and xiv
- provides guidance to consumers about how to protect their privacy when using internet-enabled devices or the IoT, and information about how to access online help.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 12:

The committee recommends that the National Plan includes, as a key priority area, ways to better coordinate intelligence gathering, data analytics, data management and investigative support services across Australian jurisdictions and agencies in order to ensure that law enforcement in Australia is able to keep pace with the rapid pace of technological change in digital communications.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 13:

The committee recommends that the Australian government considers implementing the INdata Cooperative Research Centre to address the common big data and information data sharing needs of law enforcement agencies and explores other opportunities for improving information and intelligence-sharing between law enforcement agencies in all Australian jurisdictions.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 14:

The committee recommends that the Australian government considers reviewing the *Telecommunications (Interception and Access) Act 1979* and *Surveillance Devices Act 2004* and amending them as necessary to ensure that they are technology neutral and an effective legal mechanism for meeting the telecommunications interception needs of law enforcement agencies.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.

Recommendation 15:

The committee recommends that the Australian government explores opportunities for greater engagement and partnerships with the private sector to facilitate the exchange of information and communications technology expertise and the development of novel approaches to tackling cybercrime.

Response:

The Government **notes** this recommendation. However, given the passage of time since the report was tabled, a substantive Government response is no longer appropriate.