Australian Government
Department of Home Affairs

Inquiry into the capability of law enforcement to respond to cybercrime

Parliamentary Joint Committee on Law Enforcement

10 September 2025

Introduction

The Department of Home Affairs (the Department) welcomes the opportunity to provide a supplementary submission to the re-referred Parliamentary Joint Committee on Law Enforcement (Committee) inquiry into the capability of law enforcement to respond to cybercrime.

The Department provided a submission to the Committee's inquiry on 15 December 2023 (**Attachment 1**). This submission supplements the earlier submission and evidence provided and includes updates relating to the changes in administrative arrangements that affect the responsibilities of cybercrime across government.

Cybercrime continues to significantly impact the Australian community, businesses and government services across a range of vectors, types and impact. This includes cyber-dependent and cyber-enabled crime, such as unauthorised access to data and systems, online technology-facilitated abuse and harms, and online fraud and scams.

Recent changes to the Administrative Arrangements Orders impacting cybercrime

On 13 May 2025, the Governor-General released a new Administrative Arrangements Order (AAO). Previously, cybercrime policy was the responsibility of the Attorney-General. These responsibilities have now been transferred to the Minister for Home Affairs (who is also the Minister for Cyber Security).

In practical terms, this aligns the responsibilities for cybercrime with the role the Department undertakes in terms of cyber security policy and co-ordination, and the Minister's responsibility for cyber security. It will also complement the transfer of responsibility for other relevant policy and legislation relating to law enforcement which was transferred to the Minister for Home Affairs as part of the 13 May AAO.

The Attorney-General and the Attorney-General's Department will continue to administer and have responsibility for the criminal offence framework under the *Criminal Code Act 1995*. This includes criminal offences under Parts 10.6 (telecommunications services), 10.7 (computer offences), and 10.8 (financial information offences) of that legislation.

The previous submission made by the Department in December 2023 was provided given the Department's responsibility for general cyber security policy coordination and supporting the Minister for Cyber Security.

Cyber Security Strategy 2023-2030

The Department's December 2023 submission referenced actions being taken aimed at reducing cybercrime under the 2023-2030 Australian Cyber Security Strategy (Strategy) and associated 2023-2030 Australian Cyber Security Strategy: Action Plan (Action Plan). These were Actions 3 (Disrupt and deter cyber threat actors from attacking Australia) and 4 (Work with industry to break the ransomware model). Since that time, a number of actions and initiatives have been delivered or substantially progressed.

- Cybercrime disruption activities under **Operation Aquila** (a joint operation between the Australian Federal Police and Australian Signals Directorate (ASD)) has targeted the highest priority cybercrime threats impacting Australia, both nationally and internationally, and driven global cooperation to effectively prevent, deter, and built regional capabilities to fight cybercrime in the Pacific and Southeast Asia. Several significant outcomes have been achieved under Operation Aquila, including a 30% increase in disruptive action taken against cybercriminals and enablers of cybercrime in the financial year 2024-25.
- A **mandatory no-fault, no liability ransomware reporting obligation for businesses** of at least $3m in annual turnover has been introduced by way of Part 3 of the *Cyber Security Act 2024* and has been in force since 29 May 2025.
- The Department, in close collaboration with ASD, launched a **ransomware playbook** in October 2024 on cyber.gov.au to provide information to individuals and businesses about how they can defend against, and respond from, a ransomware attack—including encouraging voluntary reporting by entities not captured under the *Cyber Security Act* obligation. Both initiatives are aimed at improving visibility of Australia's ransomware threat picture and may be used to inform future criminal law reform.

- Multiple phases of the *'Act Now. Stay Secure.'* public communications campaign have been delivered by the Department, providing the Australian public with three simple steps to improve their personal cyber security.

As the Action Plan sets out the actions for Government to take under the first two years of the Strategy (i.e. Horizon 1, 2023-25), the Department is working to develop an updated Action Plan for Horizon 2 (2026-28) including new or expanded initiatives under Actions 3 and 4. It is expected that an updated Action Plan for Horizon 2 will be released publicly in early-mid 2026.

These actions complement the 2022 National Plan to Combat Cybercrime that identifies three key pillars (Prevent and Protect, Investigate Disrupt and Prosecute, and Recover) around which to focus future action and support increased national coordination to combat cybercrime in Australia. National coordination will continue to be assisted by the Department maintaining membership to the National Cybercrime Working Group (previously referred to as Operation Helios in the Attorney-General's Department 2023 submission, **Attachment 2**).

Attachment A – Responsibilities Across Government

Department	Responsibility
Attorney-General's Department	The Attorney General's Department is responsible for Commonwealth criminal law policy (including cybercrime), identity security, privacy, critical infrastructure resilience and telecommunications interception policy. The Attorney-General's Department is also responsible for making and receiving requests to and from foreign countries to seek or provide evidence to support cybercrime investigations or prosecutions.
Australian Criminal Intelligence Commission (ACIC)	The ACIC is Australia's national criminal intelligence agency. The ACIC maintains national criminal intelligence holdings, produces strategic intelligence assessments; and coordinates national operation responses to disrupt, disable and prevent organised crime, including cybercrime, impacting on Australia
Australian Signals Directorate (ASD)	ASD works across the full spectrum of operations required of contemporary signals intelligence and security agencies: intelligence, cyber security and offensive operations in support of the Australian Government and the Australian Defence Force. ASD uses its offensive cyber capabilities to disrupt, degrade, deny and deter organised offshore cyber criminals.
Australian Federal Police (AFP)	The AFP is responsible for enforcing Commonwealth criminal law; contributing to combatting complex transnational, serious, and organised crime impacting Australia's national security; and protecting Commonwealth interests from criminal activity in Australia and overseas. AFP's cybercrime teams coordinate law enforcement responses to cybercrimes of national significance.
Australian Institute of Criminology (AIC)	The AIC is Australia's national research and knowledge centre on crime and justice. AIC informs crime and justice policy and practice in Australia by undertaking, funding and disseminating policy-relevant research of national significance.
Australian Transaction Reports and Analysis Centre (AUSTRAC)	AUSTRAC is responsible for preventing, detecting and responding to criminal abuse of the financial system to protect the community from serious and organised crime, including cybercrime. In collaboration with law enforcement partners, the national intelligence community and our regulated entities, AUSTRAC generates financial intelligence to identify, disrupt and combat cyber-enabled and cybercrime with a financial nexus, as well as cyber-enabled terrorism financing.
Commonwealth Director of Public Prosecutions (CDPP)	The CDPP is an independent prosecution service established by Parliament to prosecute alleged offences against Commonwealth law, including cybercrime.
Department of Foreign Affairs and Trade (DFAT)	DFAT leads Australia's international engagement on cyber and critical technology across the Australian Government including working across government on Australia's approach to the Cybercrime Convention.

Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA)	DITRDCA leads policy development for online safety, with the aim of supporting Australians to have safe online experiences and ensuring that there are protections in place to mitigate the risks of Australians being exposed to harmful online material.
Department of Home Affairs (Home Affairs)	Home Affairs is responsible for central coordination, and strategy and policy leadership of cyber and critical infrastructure resilience and security, immigration, border security, national security and resilience, counter-terrorism, and citizenship. Home Affairs also has principle policy responsibility for the Commonwealth Cyber Security Strategy.
The Treasury	The Treasury is responsible for the newly established National Anti-Scam Centre. Launched on 1 July 2023, the centre will build its information-sharing capabilities over the next 3 years. It will bring together experts from government and the private sector to tackle harmful scams.
eSafety Commissioner	The eSafety Commissioner is responsible for ensuring Australians have safe online experiences by developing educational resources; administering reporting and takedown schemes for cyberbullying of children, cyber abuse of adults, image-based abuse and illegal and seriously harmful online content and driving technological change.

Australian Government
Attorney-General's Department

December 2023

Parliamentary Joint Committee on Law Enforcement

The capability of law enforcement to respond to cybercrime

Attorney-General's Department Submission

Table of Contents

Overview

The Attorney-General's Department welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement (Committee) inquiry into the capability of law enforcement to respond to cybercrime.

This submission includes input from the Australian Criminal Intelligence Commission (ACIC). The Australian Federal Police (AFP), Commonwealth Director of Public Prosecutions (CDPP) and the Australian Institute of Criminology (AIC) will submit separate submissions.

The Attorney-General's Department is responsible for cybercrime policy and legislation, efforts to protect personal information under the *Privacy Act 1988*, procedural powers available to law enforcement and national security agencies, and identity security and resilience policy.

Attachment A provides an overview of Commonwealth departments and agencies with responsibilities related to combatting cybercrime.

Key points

- **Cybercrime impacting the Australian community is significantly increasing**. The harm caused is monetary and non-monetary in nature.
- **Cybercrime is diverse,** ranging from human exploitation (sexual abuse of children and adult online harms), online scams and fraud, malware and hacking, and identity theft.
- **Cybercrime often goes unreported**. When reported, the sheer scale of reported cybercrimes makes it challenging for Australian law enforcement to resource investigations.
- The **cross-border nature of cybercrime makes investigating and prosecuting cybercrime challenging.** International crime cooperation is vital to support Australian investigations and prosecutions.
- **Investment (both financial and non-financial) in domestic and international partnerships** with foreign governments, industry, civil society and international organisations, are important to Australia's ongoing efforts to combat cybercrime.
- **Cybercrime impacts all jurisdictions across Australia,** with many states and territories having their own cybercrime offence frameworks and policing resources focused on investigating those crimes.

What is cybercrime?

Cybercrime involves breaches of the criminal law. This is different to cyber security, which involves protecting government and corporate networks, and increasing the security associated with individuals using devices or software. Cybercrime continues to evolve as a result of advancements in communications technology, increased connectivity (such as Internet of Things devices), and increased engagement online (such as online shopping and access to government services).

Cybercrime can be broadly categorised as cyber-dependent and cyber-enabled crimes.

- **Cyber-dependent crimes** (e.g. computer intrusions and denial of service attacks) are crimes directed at computers or other information communications technologies.
- **Cyber-enabled crimes** (e.g. online fraud, identity crimes, child sexual exploitation and abuse) are crimes that can increase in their scale and/or reach through the use of computers, computer networks or other forms of information communication technology.

There is often overlap and co-dependency between cyber-dependent and cyber-enabled crimes. For example, computer intrusions may lead to online fraud and identity crimes. The following table provides some examples of cybercriminal activity.

Cybercrime	Explanation
Ransomware	Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files. **Impact** includes data breaches and theft, extortion. Single events can result in significant impacts to the Australian community, business and government services. Can impact critical infrastructure. **Examples**: REvil ransomware group targeting the Australian health care sector.
Business email compromise	Business email compromise is where a cybercriminal compromises an organisation via email. **Impact** includes data breaches, theft and extortion. Single events can result in significant impacts to the Australian community, business and government services. Can be a precursor to ransomware events. **Examples**: Australian financial firms being targeted through falsified invoices.
Data markets and cybercrime	Data that has been exfiltrated or otherwise obtained through cybercrime (such as unauthorised access) is often sold online. **Impact** includes personal and other identifying data being sold that facilitates identify theft, scams and further cybercriminal activity. **Examples**: Online dark web forums or markets selling Australian Tax Office and MyGov logins.
Online fraud and scams	Online scams and fraud (as cyber-enabled crime) continue to be common cybercrime types experienced by the Australian community. Online scams are becoming more sophisticated and harder for victims to identify. **Impact:** Online fraud and scams result in significant losses to those affected. Scams are impacting Australian consumers and businesses on a daily basis. Losses to scams are increasing exponentially, with an estimated $4 billion lost to scams in 2022. **Examples:** Phishing, remote access scams, identity theft, investment scams, romance scams.

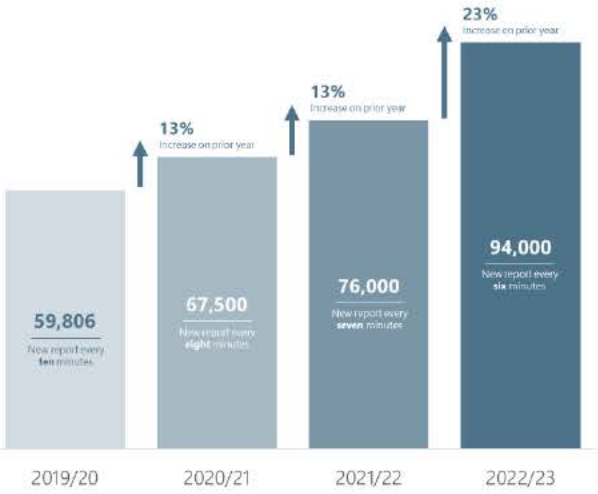
Cybercrime	Explanation
Online harms	Social media and other forms of communication on the internet continues to have significant risks of online harm. This includes cyber extortion (including adult and children sexual oriented extortion), child sexual abuse material and grooming, and harassment and bullying. **Impact:** Online harms poses significant impacts on the wellbeing and psychological health of individuals. Increasingly online harms are being monetised by organised cybercriminal groups. **Examples:** Dating applications being used to extort individuals. Creation of deep fakes.
Unauthorised access (hacking)	Unauthorised access to a system or network allows for cybercriminals to exploit a system's data or manipulate its normal behaviour. **Impact: I**ncludes data breaches and theft, extortion. Single events can result in significant impacts to the Australian community, business and government services. Can impact critical infrastructure. **Examples:** Data breaches of Medibank, Latitude, Optus and HWL Ebsworth compromised the data of millions of Australians as well as other Australian businesses and even government information.

Scale and impact of cybercrime

Individuals, businesses and governments increasingly engage online. According to the Australian Communications and Media Authority, 90% of Australian adults accessed the internet in 2019.[1] In June 2022, this figure increased to 99%. Cyber criminals increasingly exploit Australia's digital connectivity and economic prosperity for their criminal activities.

The frequency of cyber incidents is also increasing. In 2022-23 there were 94,000 cybercrime reports (1 every 6 minutes), which was a 23% increase on the previous year. The AIC's *Cybercrime in Australia 2023* report, found there is significant underreporting of cybercrime, with the community experiencing between 4.5 and 12.7 times more cybercrime than reported to police or ReportCyber. It also found that 47% of respondents had been a victim of at least one cybercrime in the past year. The average cost of cyber incidents to Australian businesses and individuals has also increased.

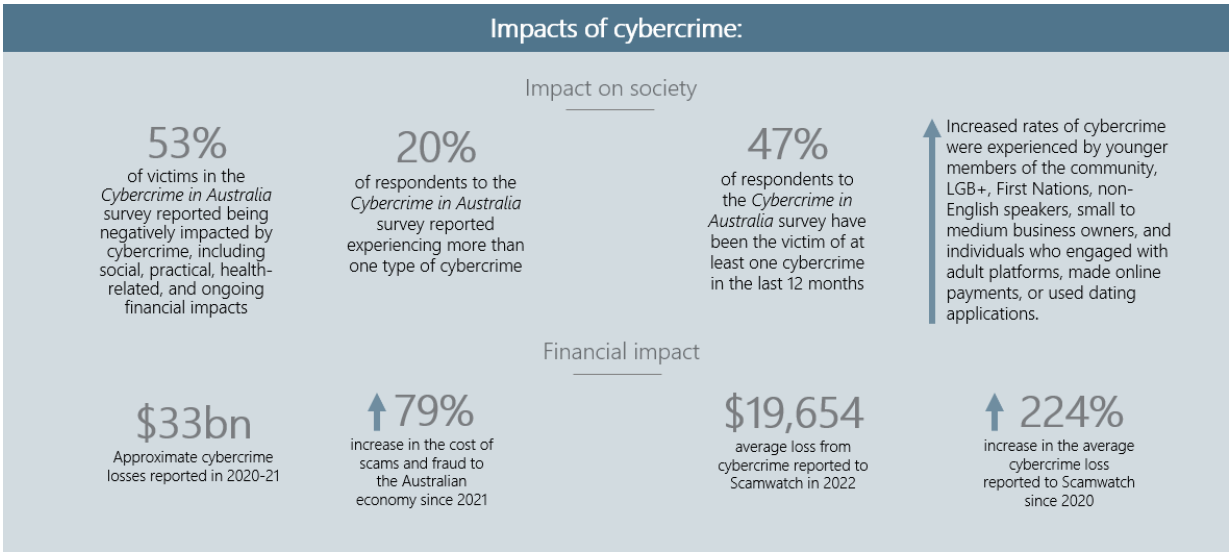
Annual cybercrimes reported to *ReportCyber*



According to the *AFP Federal Crime Threat Picture*,[2] more than $33 billion was reported as lost as a result of cybercrime in 2020-21 and this is only expected to increase.[3]

[1] Australian Communications and Media Authority, '*Communications and media in Australia series: How we use the internet*', December 2022.
[2] Australian Federal Police, '*The AFP Federal Crime Threat Picture*', July 2023.
[3] **Note:** the cost of cybercrime is difficult to quantify and there are a number of varying estimates depending on metrics used to calculate. For example, the AIC estimate the total economic impact of pure cybercrime in 2019 was approximately $3.5b.

Cybercrime can also have significant non-monetary impacts, such as reputational damage, psychological harms, financial and social stress, and disruption to the availability of business and essential services. Non-monetary impacts may also have long term impacts on individuals. For example, identity fraud and scams can result in a person being repeatedly subject to cybercrime incidents and may take significant time to restore and secure their identities. This can have a devastating impact on the ordinary lives of Australians. While some estimates of the impact of crime can be determined (such as financial loss), it can be difficult to assess the true impact of cybercrime on individuals.



Emerging threats and challenges

In Australia, the cyber threat environment continues to increase in complexity, sophistication and intensity. The key emerging threats include the use of artificial intelligence (AI), and end-to-end encryption and anonymising technologies.

Artificial intelligence

The rapid development of AI technologies in recent years presents both significant opportunities and challenges. AI is a general term that encompasses generative AI, machine learning and rules-based automation. AI allows cybercriminals to access low-cost, sophisticated products to commit crimes. Through the use of AI, scam emails are almost indistinguishable from their human made equivalents, malware can be created with little to no technical knowledge, cyber-attacks can be automated to occur at a scale previously unseen, and child abuse material can be created at prolific rates. AI can also be used to generate deep fakes (manipulated fake digital images, videos or sound files of real persons). The rapid expansion of commercial AI products and their increasingly mainstream uptake pose a risk to the Australian public, particularly where user security has not featured in the development of the product itself and regulations are not in place to protect consumers.

End-to-end encryption and anonymising technologies

End-to-end encryption and virtual private networks continue to pose challenges for law enforcement agencies. The development of such technologies is important for protecting personal information, privacy and cyber security. However, if used by malicious actors, these technologies have the potential to hide criminal activity and to interfere with law enforcement agencies' ability to prevent and respond to serious

online crime (including the collection of electronic evidence). Other technologies, such as dedicated encryption communications devices used exclusively by criminals, offer encrypted and closed network features on devices that operate outside of standard communications systems, offering anonymity to their users and impeding law enforcement's access to electronic data and communications in a meaningful format under existing warranted powers.

The Attorney-General's Department regularly engages with Five Eyes partners, large tech companies, academics and not-for-profit organisations to discuss the impacts that new and emerging technology, such as anonymising and other privacy enhancing technologies, will have on law enforcement capabilities and the challenges to lawful access to data.

Current legislative framework and policy responses

Australia has a strong framework of criminal offences and law enforcement powers, including comprehensive computer and telecommunications offences under the *Criminal Code Act 1995* (Cth) (Criminal Code). These are detailed below.

Criminal offences

The Criminal Code criminalises conduct relating to cybercrime. This includes telecommunications offences in Part 10.6, computer offences in Part 10.7, and financial information offences in Part 10.8.

Telecommunication offences (Part 10.6 of the Criminal Code)

Part 10.6 criminalises the misuse of telecommunications networks, including the internet, with maximum penalties of up to 30 years' imprisonment. Key offences include:

- **Section 474.17** – *Using a carriage service to menace, harass or cause offence* – This offence criminalises online conduct that a reasonable person would find to be menacing, harassing or offensive. There is no definition in the Criminal Code for the terms 'menace', 'harass' or 'offensive', which allows this section to consider community standards and common sense in regards to the conduct. This is a broad offence that covers a wide range of conduct online, including cyberbullying, harassment, or the extortion of individuals online. This offence is punishable by a maximum penalty of 5 years imprisonment.
- **Section 474.17A** – *Using a carriage service to menace, harass or cause offence involving private sexual materia*l – This is an aggravated offence to cover the transmission, making available, publication, distribution, advertisement or promotion of private sexual material. The offence is punishable by a maximum penalty of 7 years imprisonment.
- **Sections 474.22 – 24C** – *Offences relating to the use of carriage service for child abuse material* – These offences relate to the use of a carriage service for child abuse material including, but not limited to, possession, production, supply, transmission, and solicitation of such material. The penalties for these offences range from a maximum period of imprisonment of 15 to 30 years.
- **Sections 474.25A – 29AA** – *Offences relating to the use of carriage service involving sexual activity with, or causing harm to, person under 16* – These offences relate to the use of a carriage service to procure or groom a child under 16 years for sexual activity, groom another person to make it easier to procure a child for sexual activity, and prepare or plan to cause harm to, engage in sexual activity with, or procure for sexual activity, persons under 16 years. The penalties for these offences range from a maximum period of imprisonment of 10 to 30 years.

There are a number of other offences that target specific conduct online. These include offences relating to the use of a carriage service for suicide related material (**sections 474.29A – 29B**), and the use of a carriage service for inciting trespass, property damage, or theft, on agricultural land (**sections 474.46 – 47**), and the use of a carriage service for sharing abhorrent violent material (**sections 474.33 – 34**). These offences primarily go to criminalising cyber-enabled crime online and prevent either objectionable material being made available online, or the significant impact that the use of the internet to incite trespass on agricultural land.

Computer Offences

Part 10.7 of the Criminal Code criminalises conduct which impairs the security, integrity and reliability of computer data and electronic communications. These offences are framed in general and technology neutral language to ensure that, as technology evolves, the offences will remain applicable. For example, the term 'computer' is not defined to ensure the computer offences will encompass new developments in technology, such as mobile phones that allow access to the internet. The penalties for these offences range from a maximum period of imprisonment of 2 to 10 years. Key offences include:

- **Section 477.1** – *Unauthorised access, modification or impairment with intent to commit a serious offence* – This offence criminalises unauthorised use of computer technology to commit serious crimes, such as fraud. A serious offence is a Commonwealth, state or territory offence with a maximum penalty of five or more years imprisonment. This offence is punishable by a maximum penalty not exceeding the penalty applicable to the serious offence.
- **Section 477.2** – *Unauthorised modification of data to cause impairment* – This offence criminalises the unauthorised modification of data on a computer that would impair access to, or the reliability, security or operation of the data. For example, this offence would apply to a person who uses the internet to infect a computer with malware. This offence is punishable by a maximum penalty of 10 years' imprisonment.
- **Section 477.3** – *Unauthorised impairment of electronic communication* – This offence criminalises cyber-attacks such as denial of service attacks, where a server is inundated with a large volume of data, which is intended to impede or prevent its functioning. This offence is punishable by a maximum penalty of 10 years' imprisonment.
- **Section 478.1** – *Unauthorised access to, or modification of, restricted data* – This offence criminalises unauthorised access to or modification of data held on a computer which is restricted by an access control system. For example, this offence would apply to a person who hacks into password protected data. This offence is punishable by a maximum penalty of 2 years' imprisonment.
- **Section 478.2** – *Unauthorised impairment of data held on a computer disk* – This offence criminalises the unauthorised impairment of data held on a computer disk, credit card or other device used to store data by electronic means. For example, this offence would apply to a person who causes impairment of data by passing a magnet over a credit card. This offence is punishable by a maximum penalty of 2 years' imprisonment.
- **Section 478.3** – *Possession or control of data with intent to commit a computer offence* – This offence criminalises the possession of data (such as a program) with the intention to use that data to commit a computer offence. For example, this offence would apply where a person possesses a program which will enable them to launch a denial of service attack against a computer system. This offence is punishable by a maximum penalty of 2 years' imprisonment.
- **Section 478.4** – *Producing, supplying or obtaining data with intent to commit a computer offence* – This offence criminalises the production and/or supply of data to be used in a computer offence. For example,

this offence would apply to the sale of ransomware programs as part of a 'cybercrime-as-a-service' operation. This offence is punishable by a maximum penalty of 3 years' imprisonment.

Financial information offences

Part 10.8 of the Criminal Code covers dishonest dealings with personal financial information without the consent of the person to whom the information relates. This includes conduct such as internet banking fraud and credit card skimming. The offences are technologically neutral to remain applicable to developments in devices and techniques used to illicitly capture personal financial information. The penalties for these offences range from a maximum period of imprisonment of three to five years.

- **Section 480.4** – *Dishonestly obtaining or dealing in personal financial information* – This offence criminalises dishonestly obtaining, or dealing in, personal financial information without the consent of the person to whom the information relates. This offence is punishable by a maximum penalty of 5 years' imprisonment.
- **Section 480.5** – *Possession or control of thing with intent to dishonestly obtain or deal in personal financial information* – It is an offence for a person to possess or control anything with the intention the thing be used to commit an offence under section 480.4. This offence is punishable by a maximum penalty of 3 years' imprisonment.
- **Section 480.6** – *Importation of thing with intent to dishonestly obtain or deal in personal financial information* – This offence criminalises conduct where a person imports a thing into Australia with the intention that it will be used to commit an offence against section 480.4 or to facilitate the commission of such an offence. This offence is punishable by a maximum penalty of 3 years' imprisonment.

Review of relevant offences

Since the early 2000s, the cybercrime offence framework has been updated to respond to the ongoing and serious threat posed by online child sexual abuse, or due to emerging issues (for example, offences relating to abhorrent violent material or online incitement relating to trespass on agricultural land). However, the computer and financial information offences have largely not been amended since that time. Reform to the computer offences has primarily related to the immunities and defences available to government.

The Attorney-General's Department is currently undertaking a review of Commonwealth cybercrime offences contained within Parts 10.6, 10.7 and 10.8 of the Criminal Code. The purpose of the review is to ensure Australia's cybercrime offence framework is fit-for-purpose given the increasing and evolving threat posed by cybercriminal conduct online and to ensure there are no gaps in Australia's criminal offences for combatting cybercrime (such as responding to emerging threats identified earlier in this submission).

Under Measure 13 of the First *Commonwealth Action Plan of the National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2030*, the Attorney-General's Department is also reviewing existing Commonwealth child sexual abuse offences across the Criminal Code, including those committed using a carriage service. This measure recognises that a robust legislative framework is an important element of responding to child sexual abuse as it supports effective disruption, investigation and prosecution outcomes. The review will consider law enforcement and prosecutorial challenges and the applicability of the offences to contemporary manifestations of child sexual abuse, current and projected criminal methodologies, and advancements in technology.

Law enforcement powers

There are a range of powers across Commonwealth legislation which can be exercised by law enforcement to detect, disrupt and investigate cybercrime offences.

Legislation	Overview
Crimes Acts 1914 (Cth) (Crimes Act)	Part IAA of the Crimes Act provides powers in relation to the search and seizure of electronic data and equipment via a warrant. It allows law enforcement to, for example: • seize items found while executing a search warrant, including electronic devices • access relevant data or account-based data from seized items • use electronic equipment in order to access data that is reasonably suspected to be evidentiary material (including removing equipment, devices and copied data from premises), and • apply for an order which requires a person to provide information or assistance with accessing, copying or converting data from a computer or data storage device in order to search for and/or obtain evidential material. Part IAAC of the Crimes Act also provides for account takeover warrants which enable agencies to take control of a person's online account to gather evidence about serious offences. The actual gathering of evidence must be authorised by, and performed under, a separate authority, such as a controlled operation or computer access warrant.
Telecommunications (Interceptions and Access) Act 1979 (Cth) (TIA Act) and *Telecommunications Act 1997*	The TIA Act establishes a legislative regime for law enforcement to intercept communications in real time, and access stored communications and telecommunications data held by telecommunications providers to investigate criminal offences and other activities that threaten the safety and security of Australians. To support law enforcement, the TIA Act contains a mandatory data retention regime, which requires telecommunications providers to retain certain data sets for 2 years so that it may be lawfully accessed by law enforcement agencies as part of their investigations. The *Telecommunications Act 1997* also enables law enforcement agencies to request or compel technical advice and assistance from businesses that provide communications services.
Surveillance Devices Act 2004 (Cth) (SD Act)	The SD Act establishes a legislative regime for law enforcement agencies to use surveillance devices, including optical devices, listening devices and tracking devices, and to covertly access data held in computers through computer access warrants. The SD Act also authorises state and territory law enforcement agencies to use surveillance devices and access data held in computers under the Commonwealth regime in defined circumstances.

Legislation	Overview
	The SD Act also provides for: • Data disruption warrants enable agencies to frustrate the commission of serious offences online by modifying, adding, copying or deleting data held in computers or other devices, and • Network activity warrants enable agencies to collect intelligence on criminal networks operating online by accessing devices used by members of the criminal network.

Policy initiatives and jurisdictional coordination

The Attorney-General's Department has been progressing a number of policy initiatives, in close consultation with states and territories, to support law enforcement combat cybercrime and support industry and the community response. Key committees, forums and networks that facilitate jurisdictional coordination and information sharing are detailed at Attachment B.

National response to cybercrime

The 2022 National Plan to Combat Cybercrime (2022 National Plan) was released in March 2022 to establish a high-level strategic framework to guide national action to combat cybercrime nationally. Recognising the change in Australia's cybercrime landscape since the 2022 National Plan was released, the Attorney-General's Department is working with stakeholders to develop a new action-orientated strategic plan (the 2024 Strategic Plan) to combat cybercrime. The 2024 Strategic Plan aims to support a collaborative and effective national effort to address cybercrime through:

- detecting, preventing cybercrime and protecting the community
- investigating, disrupting and prosecuting cybercrime, and
- supporting the community to recover from cybercrime.

In developing the 2024 Strategic Plan, the Attorney-General's Department will work with stakeholders, including law enforcement, to identify capability gaps in combatting cybercrime and consider how to address them. The 2024 Strategic Plan is intended to set out actions for Commonwealth, state and territory law enforcement agencies to respond to cybercrime, protect Australia from its impacts, and build a safer, more resilient online environment for the Australian community.

National Cybercrime Capability Fund

The National Cybercrime Capability Fund (the Capability Fund) provides funding of approximately $11 million per year to Commonwealth, state and territory government entities to deliver projects that uplift national capability to combat cybercrime.

The Capability Fund supports eligible government agencies to deliver fit-for-purpose activities that aim to discover, target, investigate, disrupt, or respond to cybercrime. This may include projects that deliver specialist skill enhancement training, intelligence sharing avenues, technological innovation, cybercrime research or victim support, and research into victimology. For example, the Joint Policing Cybercrime Coordination Centre, led by the AFP, will receive up to $6.45 million over 2 years for Commonwealth, state and territory secondments to the Centre, and a prevention and outreach program. The funding uplifts

Australian law enforcement's ability to combat cybercrime by enhancing coordination and real-time intelligence sharing, and delivering nationally consistent prevention and awareness raising activities.

National Strategy for Identity Resilience

On 23 June 2023, the Data and Digital Ministers Meeting announced the release of the National Strategy for Identity Resilience to address the growing problem of identity theft. Developed in collaboration between Commonwealth, state and territory governments, the National Strategy establishes a national approach to make Australian identities resilient – hard to steal and, if compromised, easy to restore. The National Strategy contains guiding principles and practical initiatives to protect Australians from identity crime and strengthen identity security.

The National Strategy is an opportunity to:

- address long-standing issues in identity resilience
- ensure we are better prepared to respond to large data breaches
- better support victims of identity crime and scams, and
- support the digital economy and digital service delivery.

Identity Verification Services

Secure and efficient identity verification is critical to minimising the risk of cyber-enabled identity fraud and theft, and protecting people's personal information when engaging with the digital economy. The identity verification services, administered by the Attorney-General's Department, are online services that are used to compare the personal information on a person's identification document (such as an Australian passport or driver licence) against Commonwealth, state and territory government records. The key services are the Document Verification Service and the Face Verification Service.

These services provide back to source verification of government issued credentials ensuring that the credential has been genuinely issued. Back to source verification breaks models used by organised criminals who produce and sell fraudulent identity credentials on the black market.

National Strategy to Prevent and Respond to Child Sexual Abuse

The *National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2030* is a nationally coordinated, strategic framework for preventing and responding to child sexual abuse. It seeks to reduce the risk, extent and impact of child sexual abuse and related harms in Australia, and to support law enforcement and criminal justice policy outcomes.

The Attorney-General's Department notes the release of the Committee's report on its inquiry into law enforcement capabilities in relation to online child sexual exploitation on 30 November 2023, and is developing the government response.

International cooperation

International crime cooperation

Cybercrime is, by its very nature, transnational – victims, perpetrators, and evidence are often located across different jurisdictions. There are a number of inherently international challenges associated with the detection, prevention, investigation and prosecution of cybercrime. These include:

- obtaining electronic evidence across borders
- investigations may be resource intensive and there may be concerns about the success of a prosecution where extradition arrangements are not in place, and
- difficulties in identifying victims and perpetrators.

To combat cybercrime, the Attorney-General's Department works closely with foreign partners to ensure there are effective pathways to collectively share intelligence, obtain electronic evidence and cooperate. This includes cooperation to support investigations and criminal proceedings, and capacity building to ensure nation states are capable of an effective response.

Mutual legal assistance and extradition

Australia's mutual legal assistance and extradition frameworks facilitate cooperation with foreign countries where evidence, or the alleged offender, is located outside of the country seeking to prosecute the criminal conduct. The Attorney-General's Department is Australia's central authority for extradition and mutual assistance matters, and provides assistance and support to the AFP and other domestic law enforcement agencies seeking to make requests.

Extradition is the process by which one country apprehends and sends a person to another country for the purposes of criminal prosecution or to serve a prison sentence. Mutual assistance is the process by which countries provide formal government-to-government assistance in the investigation and prosecution of criminal offences and related proceedings. While these processes can involve lengthy timeframes, they assist domestic and foreign law enforcement agencies respond to and combat cybercrime. The number of requests related to cyber offences has significantly increased over the last 10 years in Australia.

International Production Order (IPO) framework

The IPO framework is a new form of international crime cooperation that will complement mutual assistance and law enforcement cooperation. This framework will enable Australian law enforcement agencies to access communications and telecommunications data directly from communications providers in foreign jurisdictions to assist in the investigation of serious crimes in Australia. It will significantly reduce the time for agencies to receive data from foreign providers and enhance the effectiveness of Australian investigation and prosecution of serious crime.

Established under Schedule 1 to the TIA Act, the IPO framework allows Australia to enter into designated international agreements with other countries to share electronic information for the purposes of countering serious crime. On 15 December 2021, Australia and the United States signed the first agreement established under the IPO framework. Following its entry into force, this agreement will enable Australian law enforcement and national security agencies to send IPOs, via the Australian Designated Authority within the Attorney-General's Department, directly to communications providers in the US such as Meta, Google and Microsoft seeking the disclosure of electronic information.

The Attorney-General's Department is working closely with key tech providers in the US, including Google, Microsoft and Meta, to facilitate the operationalisation of the IPO framework. This engagement has focused on the integration of technical systems to support the IPO framework, ensuring privacy protections are in place to protect personal information from unnecessary disclosure, and how to ensure the efficient and effective use of the IPO framework by Australian law enforcement agencies.

Regional efforts

Domestic capacity and capabilities, along with the ability to effectively cooperate internationally, are central to combatting cybercrime. The Indo-Pacific region remains particularly vulnerable to the threat posed by cybercriminals who look to exploit gaps in the region's legislative, policy, law enforcement and technical capacity.

The Attorney-General's Department works to strengthen criminal and policing frameworks in the Pacific, by supporting law and justice agencies in the region to develop and implement laws that respond to law and justice priorities, including cybercrime. In particular, Australia contributes to the Pacific Islands Law Officers' Network (PILON), a regional network of senior Pacific law and justice officials promoting justice and the rule of law, where countries share expertise and experiences to strengthen regional cooperation on key law and justice issues. Australia is a member of the PILON Cybercrime Working Group, which promotes the development and implementation of best practice legislation, evidence-gathering powers and international cooperation mechanisms for police, prosecutors and law-makers by delivering capacity-building activities in collaboration with international and regional partners.

The Attorney-General's Department also administers the Indo-Pacific Child Protection Program which aims to uplift criminal justice responses to child sexual exploitation and abuse in the Indo-Pacific region. The Program aims to develop technical knowledge and skills of law and justice officials, inter-agency coordination and cooperation, and build mechanisms to share global and regional best practice approaches to countering online and travelling sex offenders.

The Attorney-General's Department also works in partnership with officials in Pacific jurisdictions, to progress bilateral legislative reform projects which strengthen cybercrime laws and where requested, to facilitate accession to the Council of Europe Convention on Cybercrime (the Budapest Convention). The most recent example was a partnership between the Attorney-General's Department, the Government of Kiribati and Council of Europe to support the drafting and implementation of the Kiribati *Cybercrime Act 2021*.

Multilateral efforts

Australia engages in multilateral discussions on cybercrime with a view to building global standards that allow Australia, and the world, to effectively combat cybercrime. Australia also uses multilateral forums to leverage law enforcement cooperation to better combat cybercrime, seeking opportunities to shape the strategic global direction of cybercrime responses. This is increasingly important given that the complexity of the digital environment and emerging technologies has led to states developing different – and sometimes diverging – approaches to criminalisation of cybercrime, that can result in fragmentation of the legal and international cooperation landscape.

Council of Europe Convention on Cybercrime

The Budapest Convention is currently the only international treaty instrument for the purposes of combatting cybercrime and the collection of electronic evidence. The Budapest Convention enjoys considerable global membership across all continents. Australia became a signatory in 2013 and has been an active member of the Cybercrime Convention Committee since that time to share legal, institutional, law enforcement and policy experiences in combatting cybercrime domestically with other Parties to the Budapest Convention.

The Budapest Convention enhances the capability of Australian law enforcement as it provides a basis for formal international crime cooperation (such as mutual legal assistance and extradition), facilitates a global

24/7 Network of contacts across Parties, and provides a bi-annual Cybercrime Convention Committee to address emerging technologies and the ever-changing methodologies used by cybercriminals.

United Nations

The Attorney-General's Department works closely with other government departments and Australian in-country representatives to actively protect existing international law, frameworks and practices in combatting cybercrime. This includes engaging strongly with international intergovernmental organisations (such as the United Nations). Australia remains an active participant through the Crime Congress, the Commission on Crime Prevention and Criminal Justice, and efforts to negotiate a new United Nations Convention on Cybercrime. Such efforts present an opportunity to facilitate international cybercrime cooperation, support countries to criminalise cybercrime conduct and work collectively to reduce the ability for cybercriminals to take advantage of the transnational nature of cybercrime.

Engagement with industry and civil society

Institutional and legal responses to combat cybercrime, whether domestically, regionally or globally, will not be effective without effective engagement with industry and civil society. Industry are at the forefront of the efforts to combat cybercrime, whether that be through efforts to prevent companies from themselves becoming a victim of cybercrime, ensuring they have sufficient capabilities in preventing their technologies, platforms or business models being used to commit cybercrime; and providing intelligence and threat assessment services to the community. Civil society continue to have an important role to play, particularly through the research they undertake (including on protecting human rights) and the threat intelligence they generate as part of their own activities to combat cybercrime.

From a capability perspective, innovative engagement with industry and civil society can help with early detection and prevention efforts, and being able to effectively obtain electronic evidence (e.g. seeking information from industry on alleged cybercriminal activity to support investigations). The Attorney-General's Department builds strong partnerships with industry and civil society to ensure that law enforcement and capability frameworks are up-to-date and fit for purpose.

Digital industry dialogue

The Attorney-General's Department delivers an annual digital industry dialogue focussed on tackling new and emerging challenges that hinder law enforcement and criminal justice efforts to counter online child sexual exploitation and abuse.

On 10 May 2023, the annual dialogue focused on the growing issue of 'sextortion', a crime-type in which offenders often take on a false identity to coerce children into sending them self-generated child abuse material. This dialogue was attended by Meta, Snapchat, Google, Discord, TikTok and Microsoft alongside AFP officers who are responsible for investigations, intelligence and triage. The dialogue was an opportunity for law enforcement and digital industry to build strategic partnerships, discuss the challenges they face, talk about the expectations on industry, and share intelligence and information.

Following significant interest and positive feedback from industry, a second dialogue was delivered on 14-15 November 2023 focussing on the rise of AI, and impacts on online child sexual exploitation and abuse.

Policy and legislative reform

Privacy Act Review

The security and destruction of personal information are areas of increasing concern, particularly with the advancement of technology and the way Australians utilise digital products and platforms. The volume of data flowing through digital ecosystems increases the risk of data breaches, including those involving malicious or criminal attacks. This often involves significant harm associated with identity scams and fraud.

Australia's privacy framework is critical to the protection of personal information and regulating how such personal information should be protected. On 28 September 2023, the Attorney-General released the government's response to the *Privacy Act Review Report*, which committed to uplifting privacy protections while encouraging digital innovation. The Attorney General's Department is progressing reforms relating to deleting or de-identifying personal information, which are designed to better protect this information and prevent identity scams and fraud while balancing the needs of law enforcement to access and obtain evidence for prosecutions. The relevant proposals include:

- a right to erasure (proposal 18.3), subject to exceptions (proposal 18.6) including competing public interests, where complying with the request would be contrary to other laws, and where technically impossible or unreasonable. In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement,
- additional guidance on when and how entities must destroy/de-identify information (proposal 21.5), and
- a Commonwealth review of data retention provisions (proposal 21.6).

Electronic surveillance reform

Electronic surveillance powers are a significant tool for law enforcement agencies to investigate criminal activity and other threats, including cybercrime. Given the increasing use of electronic communications by criminals and other malicious actors, and the fact that this offending is conducted in large parts (and sometimes entirely) online, electronic surveillance powers are particularly vital to the investigation and prosecution of these crimes.

The Attorney-General's Department is currently leading a major legislative reform project to develop a new, more robust Commonwealth electronic surveillance framework as recommended by the *Comprehensive Review of the legal framework governing the National Intelligence Community.* The reforms would repeal the TIA Act, SD Act and parts of the *Australian Security Intelligence Organisation Act 1979* (Cth), and replace them with a single Act. The new Act would establish a modern and comprehensive framework for lawful access to information to respond to serious crime and national security threats including cybercrime.

Anti-money laundering and counter-terrorism financing reform

The government has announced consultation on major reforms to Australia's anti-money laundering and counter-terrorism framework. The reforms will ensure Australia's laws meet international standards and keep pace with the evolving threat environment. They will include extending the current regime to additional services provided by digital currency exchange providers, commonly known as cryptocurrency or virtual asset exchanges, as these providers are at heightened risk of exploitation by cybercriminals seeking to use their platforms to disguise the origin of funds.