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.