Australia Post

1 March 2024
Department of Home Affairs
Submitted online

Response to the 2023-30 Cyber Security Strategy

Australia Post appreciates the opportunity to respond to the Department of Home Affairs consultation on the 2023-2030 Australian Cyber Security Strategy (the Strategy). We thank the Department for its collaborative approach to the development of this strategy and look forward to continued involvement in this process.

Cyber security is a critical issue for customers, businesses, and government. A clear strategy based on transparency and coordination are fundamental to ensuring early identification, cooperation, and risk reduction for Australians. As such, Australia Post supports the development of the Strategy. Australia Post also encourages ongoing work to harmonise cyber security, privacy, data management and identity policy and regulatory regimes. These areas are closely connected, for example through data retention and storage requirements.

We support the Strategy's acknowledgement of the vital roles that existing bodies play, and will continue to play in cyber security, including the Australian Signals Directorate (ASD), the Australian Cyber Security Centre (ACSC), and the Australian Federal Police (AFP). Coordination amongst these bodies, and other relevant regulators, will be critical for minimising regulatory overlap and ensuring proportionate and effective reporting obligations for businesses.

In the event of an incident, it is important that impacted businesses can have a single window for reporting. The ACSC, given its existing role involving cyber reporting functions, would serve as a logical central reporting point for incidents. The body acting as the single-window would then ensure that all other relevant departments and regulatory bodies are notified of the information specific to their needs (i.e., on a strict as-needed-basis) to ensure confidentiality and to allow businesses to focus on incident management.

In relation to ransomware specifically, we encourage the Department to consider a light-touch approach to information required in the initial report by impacted businesses. This would allow for notification at the point of identification and allow the business more time to investigate for additional information as outlined in the Strategy. A rigid timeframe for specific information may be challenging, as incidents could extend over weeks or months. As such, a no-fault no-liability approach principle for ransomware reporting would encourage businesses to engage in the framework in a collaborative way.

It would be useful for industry to receive anonymised information on indicators of compromise, along with Tactics, Techniques and Procedures which should be disseminated wisely and swiftly following a ransomware incident. This will enable organisations to update their threat detection

tools and conduct through searches across their systems to ensure they are not being targeted by the same threat actor.

To discuss this feedback in more detail, please contact Kat Burela, Head of Industry, Policy, and Regulatory Affairs at [redacted].