Australian Government
Australian Signals Directorate

ASD

Select Committee on Foreign Interference through Social Media

ASD Submission

Introduction

The Australian Signals Directorate (ASD) welcomes the opportunity to provide a written submission to the Select Committee on Foreign Interference through Social Media. This submission has been prepared with regard to the following Terms of Reference of the committee:

> *b. responses to mitigate the risk posed to Australia's democracy and values, including by the Australian Government and social media platforms;*

ASD's role

As set out in the *Intelligence Services Act 2001*, one of ASD's functions is to provide material, advice and assistance relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means. Through this function, ASD provides advice to Australians on matters relating to the technical security of social media and messaging applications (apps). ASD publishes this advice on its Australian Cyber Security Centre's website (cyber.gov.au).

ASD's advice is designed to both highlight the security risks to consider when using social media and messaging apps, and to provide practical guidance on how individuals, businesses, and entities can enhance the security and privacy of their social media accounts and applications.

It is important to note that ASD does not review or assess the cyber security status of specific social media or messaging applications. Nor does ASD have a regulatory role in relation to these technologies.

Risks associated with social media and messaging apps

Social media and messaging apps can pose risks to the security and privacy of individuals and organisations. Broadly, ASD views the potential risks associated with social media and messaging apps as being:

i. exploitation of personal information posted to social media, or shared via messaging apps. Specifically, such information can be used in extortion or social engineering campaigns that aim to elicit other sensitive information that, in turn, can be used to compromise an individual's or organisations systems and networks.

ii. extensive data collection and possible storage and access of that data outside Australia. Social media and messaging apps typically collect extensive data as part of their business model. These apps may also collect additional data from individuals' devices, which extends beyond content of messages, videos and voice recordings. The type of data collected may change over time, including when new versions or features are released. Terms of use and privacy policies relating to what data is collected, how and when it can be used, may also change at short notice or be difficult to understand. Sometimes this data is stored outside of Australia and may be subject to lawful access or covert collection by other countries. In such cases, Australian legislation and privacy or consumer laws may not apply.

iii. identity theft, fraud, and reputational damage. Social media and messaging apps are a common way for an adversary to gather information on individuals as well as organisations' activities and systems. When personal or sensitive information is posted to social media, or shared via messaging apps, this has the potential to cause reputational damage. Information that appears to be benign in isolation could, if aggregated with other information, breach users' privacy.

These risks are discussed further in ASD's *Security Tips for Social Media and Messaging Apps* publication on cyber.gov.au.

ASD's support to electoral integrity

ASD supports the integrity and resilience of Australia's democracy through the provision of cyber security advice to federal, state and territory electoral bodies.

In the lead up to the 2022 Federal Election, ASD supported the Australian Electoral Commission (AEC) through the Electoral Integrity Assurance Taskforce, by providing:

- cyber security threat intelligence briefings
- technical advice and assistance
- hunt activities to identify malicious activity on AEC systems
- system vulnerability assessments of AEC network technical settings and controls, and
- enhanced cyber incident response support.

In relation to state and territory elections, ASD provides the relevant electoral bodies:

- bespoke technical advice in the lead up to and during an election
- incident response support on election day through the Australian Cyber Security Centre's 24/7 Hotline
- a state or territory-specific strategic cyber security threat assessment, and
- network monitoring capabilities, including host based sensors.

In the lead up to the 2022 Federal Election, ASD also provided Australia's political parties with cyber threat briefings and tailored advice. ASD encouraged politicians and their staffers to implement cyber security practices to enhance their cyber resilience through:

- updating and patching operating systems
- updating and patching software and apps
- enabling multi-factor authentication, and
- backing up important files.

This advice is further discussed in ASD's *Cyber Security Guide for Politicians and Staff - 2022 Federal Election* publication.

Cyber Supply Chain Risk Management and High Risk Vendors

ASD provides advice to government and Australian business on cyber supply chain risk management. Australian organisations should consider cyber supply chain risk management as part of their business as usual operations, including in relation to their use of social media applications.

ASD advises individuals and organisations to consider the issues below when identifying risks associated with their use of suppliers, manufacturers, distributors and retailers:

- nationality of suppliers
- foreign control, when a supplier may be subject to foreign laws which may conflict with Australian laws or interests, and
- foreign influence and interference, when a foreign government attempts to influence Australian society in a way that benefits their interests.

These risks are discussed in ASD's *Identifying Cyber Supply Chain Risks* publication on cyber.gov.au.

These mitigations and risks should also be considered in the context of selecting software and technology products for critical business functions and systems containing sensitive data.

February 2023