Australian Government

Electoral Integrity Assurance Taskforce

Election Security Environment Overview

As set out in the Electoral Integrity Assurance Taskforce's (EIAT) Terms of Reference, the purpose of the EIAT is to provide consolidated and coordinated information and advice to the Australian Electoral Commissioner on matters that may compromise the real or perceived integrity of a federal electoral event, which includes elections, by-elections and referendums.

Threats to the integrity of Australia's electoral system may be realised through various vectors, including a cyber-or physical security incident, foreign interference and the spread of mis/disinformation. This document provides an overview in relation to these areas.

Foreign interference

Experiences from democracies around the world, show that elections are not immune from foreign interference. Some foreign powers are interested in impacting the real or perceived legitimacy of results; others seek to undermine the concept of democracy itself. Some foreign powers target candidates directly or, through the spread of disinformation, the voting public.

It is possible that foreign powers may seek to undertake similar actions in Australia. While attempts to interfere in our democratic processes are common, successful interference is not. Our democracy remains robust, our parliaments remain sovereign, and our elections remain free and fair.

Foreign interference is a more prolific threat than ever before. Individuals or groups engaging in these actions, and those assisting them are often difficult to identify, and their links to foreign powers may not be immediately apparent.

Foreign interference is illegal. It is an activity carried out by, on behalf of, directed or subsidised by, or undertaken in active collaboration with a foreign power, and either involves a threat to a person, or is clandestine or deceptive and detrimental to Australia's interests.

Australia has a mature framework to ensure our institutions and communities are resilient to foreign interference. This includes measures to protect our democracy and uphold our laws and values, such as robust criminal offences and the Counter-Foreign Interference Taskforce, which leads Australia's operational response to espionage and foreign interference.

Physical security

Ensuring Australians remain safe is the primary concern of all Australian governments, and a shared, collaborative effort.

Protest activity

Peaceful protest is an important and a treasured democratic right in Australia. But provocative or disruptive activity intended to prevent people from exercising their right to vote is fundamentally anti-democratic. Challenges to social cohesion and wider acceptance of conspiracy theories can create an incubating environment for grievance to develop, but it remains important that the process of elections not become the target for these grievances.

Over the past few years, large-scale anti-government protests have emerged globally, motivated by a range of political, economic, and social factors. Domestically, anti-government rhetoric and threats (online, targeted or opportunistic) towards federal parliamentarians and government figureheads have significantly increased since 2021. The AFP has seen an escalation of criminal activities targeting federal parliamentarians which includes damage to federal parliamentarian electorate offices, threats and intimidation.

The AFP works with state and territory police to ensure the safety of parliamentarians and the wider community. The ability of parliamentarians to discharge their duties without fear of harm underpins Australian democracy.

Terrorism

The security environment in Australia is complex, challenging, and changing. The terrorism threat level is PROBABLE.

A growing number of Australians are being radicalised to violence and radicalised to violence more quickly. More Australians are embracing a diverse range of extreme ideologies and a willingness to use violence to advance their cause. Australia is witnessing an increase in anti-government and anti-authority extremism, and the use of emerging technologies to enable, produce, disseminate and amplify messages of hate and violence at an unprecedented scale and pace.

Australia's response to the threat of terrorism is multi-faceted, supported by mature Australia-New Zealand Counter-Terrorism Committee (ANZCTC) frameworks, inter-agency partnerships and expertise. The Commonwealth Counter-Terrorism Coordinator chairs the ANZCTC, which fosters partnerships across governments, internationally, with communities and the private sector. The ANZCTC's National Counter-Terrorism Plan outlines arrangements, governance and operational responsibilities in this context. National Guidelines for Crowded Places provide important advice for owners and operators of crowded and public venues to ensure the safety of their locations. Joint Counter Terrorism Teams (JCTTs) exist in all states and territories of Australia and consist of the AFP, the relevant State or Territory Police, ASIO and, in NSW, the NSW Crime Commission. Their primary objective is the prevention and disruption of terrorism and the protection of Australians and Australian interests. Where a terrorism nexus is identified, the JCTTs will act to disrupt any individuals that pose a risk to the Australian community.

The JCTTs are experienced in managing complex and sensitive terrorism investigations, with the JCTT construct being mature, having been developed and tested over many years.

Cyber security

While technological advancements continue to benefit Australia's social and economic prosperity, they also enhance the capabilities of malicious cyber actors, increasing the potential frequency and severity of cyber attacks and incidents.

An increasingly digital world increases the risks to national security and personal data security. The Australian federal election may attract a level of interest from malicious cyber actors, including state-sponsored actors, cybercriminals and hacktivists, whom may have the intention to disrupt, interfere with, or undermine the conduct of the 2025 Australian federal election.

Globally, malicious actors have demonstrated a capability and willingness to target election infrastructure and high-profile individuals. They use a range of methods to disrupt, influence, gain access to sensitive or classified data, including through phishing, information stealer malware and doxing.

The government works with appropriate Commonwealth, State and Territory agencies to constantly review cyber threats and mitigate cyber security risks. The Australian Signals Directorate (ASD)'s Annual Cyber Threat Report 2023-2024 states that Australia's challenging cyber threat landscape has led to regular targeting of networks by malicious cyber actors, both deliberately and opportunistically. ASD provides cyber security advice and technical assistance to protect systems, accounts, devices and data at cyber.gov.au.

Misinformation and disinformation

Voters have access to an ever-increasing number of sources of news and information – but not all of it is trustworthy. Australians can expect there will be more misinformation and disinformation during elections, particularly online.

- Misinformation is false, misleading or deceptive information, that is spread due to ignorance, by error or mistake, or without the intent to deceive. It can include made-up news articles, doctored images and videos and false information shared on social media.
- Disinformation is the deliberate spread of false information to deceive or mislead for malicious or deceptive purposes. This can cause confusion and undermine trust in government and institutions.

While disinformation directed covertly by a foreign power is foreign interference, most disinformation does not involve a foreign power. The shifting online environment involves the use of inauthentic activity to try and influence public debate, and generative artificial intelligence to produce false narratives, fake images and deepfake audio and videos, requiring all Australians to think deeply about what they are reading, hearing and watching, and to stop and consider the source of information. This is a particularly important consideration when weighing up voting decisions.

To support voters during the 2025 federal election, the Australian Electoral Commission will again provide resources to voters, including its digital media literacy campaign, Stop and Consider.

Reporting suspicious behaviour

The public plays a major role in providing information to law enforcement and security agencies about possible national security threats, including terrorism and foreign interference. If you believe you have information, have seen or heard something suspicious that may need to be investigated by security agencies please contact the National Security Hotline via:

Phone the National Security Hotline on 1800 123 400
(operating 24 hours a day, 7 days a week) or +61 1300 123 401 (if you are outside Australia)

If you require an interpreter, you can call the Translating and Interpreting Service on 131 450 (if in Australia). You can ask them to call the National Security Hotline on 1800 123 400

SMS: 0498 562 549 **Email:** hotline@nationalsecurity.gov.au

Web form to the Australian Federal Police (AFP) by filing a Commonwealth Crime Report on their website https://forms.afp.gov.au/online_forms/report-commonwealth-crime

If the incident involves serious online abuse, you can also make a report to the eSafety Commissioner at esafety.gov.au/report

If you are impacted by a cyber incident or cybercrime, you can report it at cyber.gov.au or contact the Australian Cyber Security Hotline on 1300CYBER1 (1300 292 371).

If there is an immediate threat to your safety call 000.

January 2025