AFP AUSTRALIAN FEDERAL POLICE

POLICING FOR A SAFER AUSTRALIA

FACTSHEET

Foreign Interference in the Community

How to report threats and intimidation from foreign governments

Introduction

Foreign interference represents a serious threat to Australia's people, sovereignty and security, and the integrity of our national institutions. Threats of foreign interference are not constrained to one sector of the Australian community nor perpetrated by a single nation-state. Hostile foreign state actors (countries that undertake hostile activity against other countries) are creating and pursuing opportunities to interfere with Australian decision-makers at all levels of government and across a range of sectors, including: democratic institutions; education and research; media and communications; critical infrastructure; and importantly, our culturally and linguistically diverse (CALD) communities.

Foreign interference in the community

Foreign interference in the community is defined as threats and intimidation directed, supervised or financed by foreign governments and targeted towards CALD communities in order to cause harm and impact on Australia's multicultural way of life. Foreign governments may interfere in communities for a range of purposes:

- to silence criticism of the foreign government's internal and external policies
- to monitor the activities (offline and online) of members of CALD groups
- to promote the views and policies of the foreign government
- to obtain information for the benefit of the foreign government
- to influence the views and opinions of the broader population.

Foreign interference in the community may take many forms

Including:

- Assault or threats of assault
- Blackmail
- Kidnapping, unlawful detainment or deprivation of liberty
- Stalking and unwanted physical or electronic surveillance
- Coercion of an individual by threatening their family or associates overseas to force them to comply
- Online disinformation campaigns through social media to discredit an individual or group.

Importantly, to constitute foreign interference under the *Criminal Code Act 1995* (Cth), the activity **must** be linked to a foreign government or its proxy. In assessing criminality, law enforcement agencies may also consider Australian State or Territory offences.

Who is targeted?

Foreign governments may target:

- Former or current nationals residing in Australia
- Political and human rights activists
- Dissidents
- Journalists
- Political opponents
- Religious or ethnic minority groups.

What can I do to help?

While not all reports of foreign interference in the community will generate an obvious AFP response, each report **helps to build a picture** of emerging issues.

Any concerns and/or instances of foreign interference in the community can be reported to the **National Security Hotline (NSH).**

- The NSH operates 24 hours a day, 7 days a week and is the central point of contact to report concerns about possible foreign interference in the community.
- NSH operators will know what to do with the information you provide, and where appropriate, they will pass it on to law enforcement and security agencies for assessment.
- NSH operators take each call seriously and value all information received.
- We know that reporting a matter of concern can be a big step. We take your right to privacy seriously. Please tell the operator if you want to remain anonymous.
- Due to the sensitive nature of the information, you will not receive advice on the outcome of your call or email.

The information you provide may be the missing piece the AFP needs to help prevent foreign interference in the community.

There are several ways to contact the **NSH:**

- **Call: 1800 123 400**
  - From outside Australia: (+61) 1300 123 401
  - For TTY users (hearing impaired users): 1800 234 889
  - **If you need an interpreter, please call the Translating and Interpreting Service on 131 450 and ask them to call the National Security Hotline**
- **SMS:**
  - Please send your information via text message to 0429 771 822
- **Email:**
  - Please send your information via email to: hotline@nationalsecurity.gov.au
- **Post**:
  - Please post your information to:
    National Security Hotline
    Department of Home Affairs
    PO Box 25
    Belconnen ACT 2616

Other ways to report

You can also report your concerns via a range of other means where appropriate.

- eSafety helps remove seriously abusive online content. You can report **serious online abuse** to the eSafety Commissioner at www.esafety.gov.au/report.
- If you feel **threatened or unsafe** in any way**,** you can contact**:**
    - **The police - on 000 for immediate threats**
    - **The police - on 13 14 44 for police attendance at non-life threatening incidents.**
- You can report a Commonwealth crime to the AFP via an online Report a Commonwealth Crime form at https://forms.afp.gov.au/online_forms/report_a_crime. For more information on what constitutes a Commonwealth Crime, please see https://www.afp.gov.au/contact-us/report-commonwealth-crime#What-is-a-Commonwealth-crime.
- Any member of the community can report suspected espionage or foreign interference activities by speaking directly to a member of the AFP (including the AFP's Community Liaison Team).

What can I expect by reporting foreign interference in the community?

The AFP cannot investigate every report of foreign interference in the community. Each call to the NSH or report of crime is assessed on a case-by-case basis to determine if any criminal offending is identified. Outcomes of making a report include:

- there may be no response because the matter does not meet a legislative threshold for police to take action
- the AFP may investigate
- another police service or government agency may deal with the matter.

For offences that occur outside Australia, jurisdictional limitations apply.

Types of threats

If you are threatened in person

- Write down or record the threat exactly as it was communicated.
- Record as many descriptive details about the person who made the threat (name, gender, height, weight, hair and eye colour, voice, clothing, or any other distinguishing features).
- Report the threat to police.

If you are threatened over the telephone

- If possible, signal others nearby to listen and notify police.
- Record the call if possible.
- Write down the exact wording of the threat.
- Copy any information from the phone's electronic display.
- Be available to discuss the details with police.

If you are threatened via electronic means including over text message, direct/private message, social media or email

- Do not delete the messages.

- Print, photograph, screenshot, or copy the message information (subject line, date, time, sender, etc.). Be sure to save or take a screenshot of messages designed to be temporary.
- Immediately notify police that you have received a threat.
- Preserve all electronic evidence.

To protect yourself from these types of threats, follow these tips:

- Do not open electronic messages or attachments from unknown senders
- Do not communicate on social media with unknown or unsolicited individuals
- Make sure your security settings on your devices/accounts are set to the highest level of protection
- Cyber criminals can compromise your electronic devices and expose personal information
- Immediately contact your financial institutions to protect your accounts from identity theft
- Use strong passphrases and do not use the same passphrase for multiple websites
- Ensure anti-virus and anti-malware applications are up to date
- Apply system and software updates as required
- Apply two-factor authentication
- Backup data regularly
- Secure your mobile device
- Develop your Cyber Secure thinking and awareness
- For more information, visit www.cyber.gov.au.