Australian Government

EIAT
Electoral Integrity Assurance Taskforce

A CANDIDATE'S GUIDE TO THE CHANGING ELECTORAL ENVIRONMENT

MAINTAINING AWARENESS AND STAYING SAFE

TABLE OF CONTENTS

IMPORTANT CONTACT DETAILS

The Australian Electoral Commission (AEC):
Phone: 13 23 26
Email: info@aec.gov.au

Australian Communications and Media Authority (ACMA):
Phone: 1300 850 115
Making a complaint

eSafety Commissioner (eSafety):
Report online harm [e.g. Adult cyber abuse scheme]

National Security Hotline (NSH):
Phone: 1800 123 400
SMS: 0429 771 822
Email: hotline@nationalsecurity.gov.au

Australian Signals Directorate (ASD)
Australian Cyber Security Centre (ACSC):
Phone: 1300 CYBER1 (**1300 292 371**)
Reporting avenues and recovery advice

CALL 000 FOR IMMEDIATE THREATS | For non-life-threatening incidents, call 131 444

Australian Government

EIAT
Electoral Integrity Assurance Taskforce

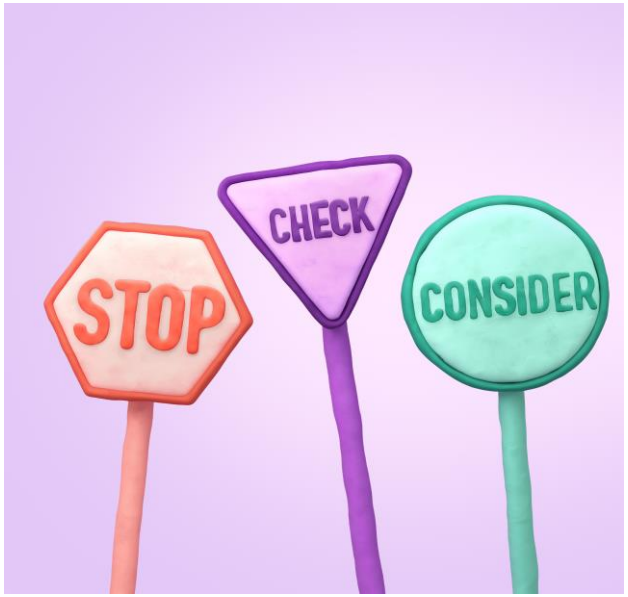
MISINFORMATION, DISINFORMATION, AND THE ONLINE ENVIRONMENT

DISINFORMATION AND RELATED TERMS

- Definitions of misinformation, disinformation, and malinformation are available on the ACMA website.
- The AEC is the authority on the federal electoral process, and keeps a disinformation register to debunk electoral mis and disinformation.
- You can also find information on foreign information manipulation and interference, otherwise known as FIMI, on the European Union External Action (EEAS) website.
- Phishing is a way malicious actors trick you into giving them personal information; find out more on the ASD's Australian Cyber Security Centre website.
- Spoofing is a method malicious actors use in which they pretend to be someone they are not.

The AEC is not the arbiter of truth in political advertising

TRUSTED ELECTORAL INFORMATION AND WHERE TO FIND IT



AEC's Stop and Consider Campaign

During a federal election there is a large amount of information being distributed online. Some of this may be false or misleading.

- **There are many tactics that may be used to attempt to mislead you.**
- If you're unsure, the AEC is the authoritative source of truth for electoral information.
- Follow the AEC on social media to stay well informed:

AEC | @AusElectoralCom | @auselectoralcom | @AusElectoralCom | AEC TV | @auselectoralcom

If you see anything the AEC would want to know about, this includes content that is impersonating, threatening or harassing the AEC or their staff, or contains incorrect information about the electoral process, please let the AEC know by direct message or tagging them.

You can also submit a complaint to the AEC or contact 13 23 26.

For matters unrelated to the AEC, you may consider reporting content to social media platforms that, for example:

- impersonates someone,
- has inappropriate comments, or
- is harassment or bullying.

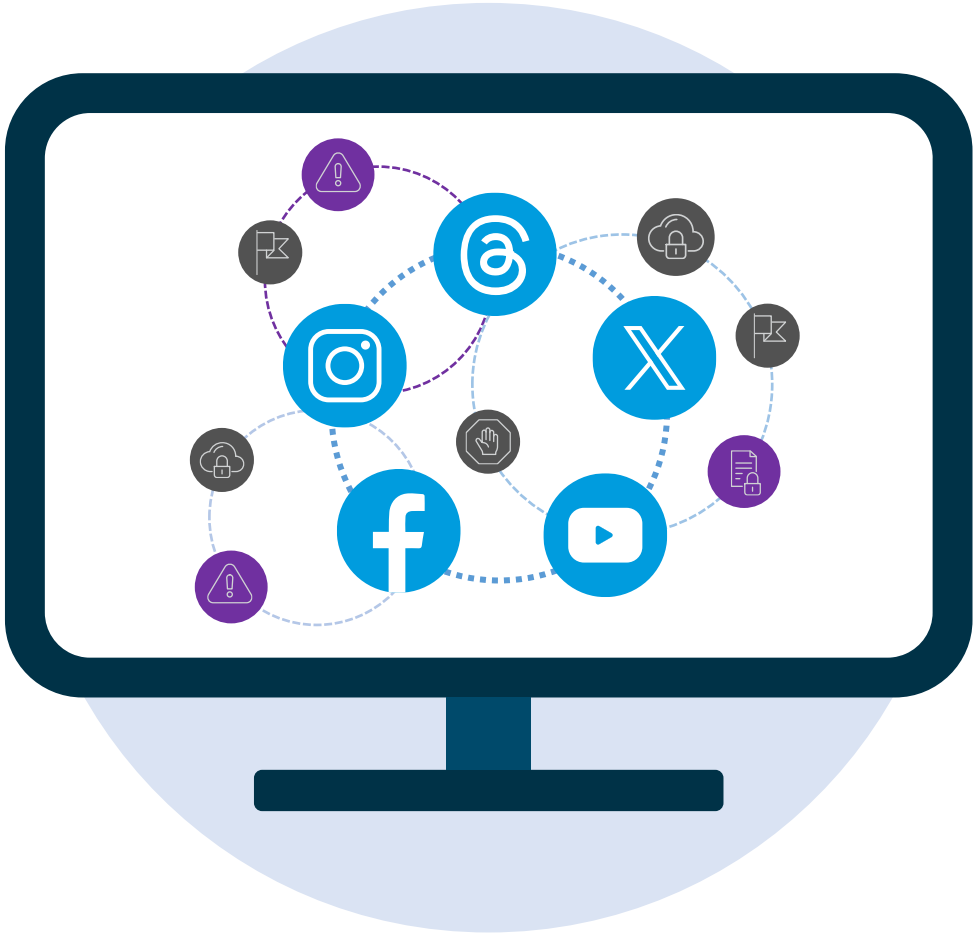
Serious threats of violence or harm should be directly reported to the eSafety Commission and local police.

ONLINE PLATFORMS ESCALATION

The various online social media platforms all have avenues for reporting content or escalating a previous report. Some examples of the mainstream platforms are Facebook, Instagram, YouTube, X (formerly Twitter), and TikTok.

Meta (Facebook, Instagram, Threads) also have a candidate guide.

For serious cases of threats, intimidation or harassment contact the eSafety Commissioner and your state or territory police service.



REPORTING AND ACCESSING SUPPORT FOR ADULT CYBER ABUSE

For information on adult cyber abuse, what it is and how to report it, please refer to the eSafety Commissioner's website.

For information on the Women in the Spotlight program, which offers social media self-defence training on how to use online services and platforms more safely and effectively, please refer to the eSafety Commissioner's website.

Australian Government

EIAT
Electoral Integrity Assurance Taskforce

CYBER SECURITY

PROTECTING YOURSELF ONLINE

Software and apps can hold sensitive information such as messages, credit card details and photos. Protect your information by regularly updating and patching your software and apps.

Find out more on how to protect yourself:

- Update your device and software
- Turn on multi-factor authentication (MFA)
- Create strong and unique passphrases
- Back up your files and devices

Here are more security tips for personal devices and tips on how to secure your social media.

REPORTING CYBER INCIDENTS

Cyber security incidents can be reported to the Australian Cyber Security Hotline on 1300 CYBER1 (**1300 292 371**). This service operates 24 hours a day, seven days a week. Additionally:

- If you think you have been the victim of a cyber-attack you should speak to your IT support team straight away.
- The sooner they know, the sooner they are able to help you.

Find out more on ASD's website at www.cyber.gov.au.

Australian Government

EIAT
Electoral Integrity Assurance Taskforce

COUNTERING FOREIGN INTERFERENCE

HOW YOU MIGHT BE TARGETED

Foreign interference is 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.

Individuals or groups engaging in foreign interference and espionage, and those assisting them, may not be readily identifiable, and their links to foreign governments may not be apparent.

The following activities are frequently used to make targeted individuals feel a sense of obligation:

- Gifts
- Donations
- Expenses-paid travel
- Networking opportunities
- Preferential access to senior officials or business people.

While cultivation attempts can be very subtle, particularly in the initial stages, they may also be much more direct and coercive.

HOW YOU MIGHT BE TARGETED

Cultivation
Foreign governments may attempt to develop relationships with you and your staff, with the aim to exert influence over you. They may covertly target your friends and family to obtain information that could be used to their advantage.

Infiltration of your office
Foreign governments could employ a number of methods to covertly gain access to sensitive information and decision makers through your office, including the compromise of your staff (insider threat).

Information operations
Foreign governments could manipulate information or post disinformation at scale and without attribution to themselves to exacerbate community tension or influence voter sentiment and the outcome of an election. This might occur in the form of generative-AI or coordinated inauthentic networks.

Undeclared donation source
Foreign governments may seek to circumvent election funding laws by donating money or providing other financial incentives in return for access and the potential for undue influence on future decision making and policy development if you are elected.

More information about what foreign interference is, how to identify it, and what support is available can be found online.

HOW TO PROTECT YOURSELF

- Be alert to unusual questions or requests for contact that is suspicious, ongoing, unusual or persistent (SOUP).
- Be mindful of your own vulnerabilities and consider whether your engagement with a particular individual could leave you compromised – now or in the future.
- Check the validity of any gift or donation offers you receive. The AEC provides detailed information for candidates on its website which includes information on election funding and financial disclosure obligations under Australian electoral law.
- Be mindful of the conversations you are having, where they are held and those who are present.
- Be aware of the information about yourself that you make available to the public, for example, through social media or other online platforms – this information may be used by foreign governments to target you.
- Report any concerning behaviour of foreign diplomats or consular officials, in their engagement with you or with the broader Australian community.

REPORTING SUSPECTED FOREIGN INTERFERENCE

If you believe you may have information on possible foreign interference activity, or have seen or heard something suspicious contact the **National Security Hotline:**

- **Phone**: 1800 123 400
- **Email**: hotline@nationalsecurity.gov.au
- **SMS**: 0429 771 822
- **Mail:** National Security Hotline
  Department of Home Affairs
  PO Box 25
  Belconnen ACT 2812

The National Security Hotline operates 24/7. The officers take every call seriously and you can remain anonymous if you wish.

For more information, visit the Home Affairs Counter Foreign Interference website.

For any queries regarding the behaviour of foreign diplomats or consular officials, please contact the Department of Foreign Affairs and Trade's Protocol Branch.

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

FOREIGN INFLUENCE TRANSPARENCY SCHEME

As a candidate for elected office, you or associated staffers may have obligations under the Foreign Influence Transparency Scheme to register certain activities.

Registration obligations

Individuals may be required to register under the scheme if they undertake, or enter into an arrangement to undertake, certain 'registrable activities' on behalf of a 'foreign principal' for the purpose of political or governmental influence.

'Registrable activities' include; parliamentary or general political lobbying, communications activities, and disbursement activity.

A 'foreign principal' includes a foreign government, foreign political organisation, foreign government-related entity, and foreign government-related individual.

If you believe you may have obligations to register under the Scheme, you can contact the Attorney-General's Department for more information. It is also open to you to seek professional legal advice on your potential obligations under the Scheme.

It is an offence to knowingly fail to register if required under the Scheme.

You may register online at the Foreign Influence Transparency Scheme Portal.

Further information can be found on the Foreign Influence Transparency Scheme website.

Australian Government

EIAT
Electoral Integrity
Assurance Taskforce

SAFETY AND SECURITY

PERSONAL SAFETY

The following states and territories police services have advice on their websites: QPOL, NSWPOL, SAPOL, WAPOL, VICPOL, TASPOL, NTPOL, ACT Policing.

The AFP provide guidance on security awareness to parliamentarians and their staff which includes through the provision of the 'Stay Secure' information. The AFP's Security Protection Diplomatic Liaison teams in the relevant State or Territory can be contacted for further information.

If you feel threatened or unsafe in anyway, contact:

- The police – on 000 for immediate threats
- The police – on 131 444 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.

- Find out more about what a Commonwealth crime is.

You can report issues that might pose a threat to national security, including suspected terrorism, to the National Security Hotline – on 1800 123 400.

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.

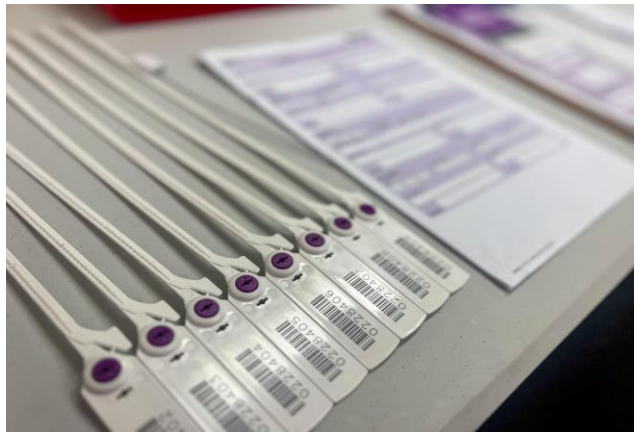
If you are threatened over the telephone

- 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.

BALLOT PAPER SECURITY



From printing through to statutorily authorised destruction, ballot papers are handled securely by the AEC through strictly codified chain of custody and security measures.

The AEC takes the security and custody of ballot papers very seriously. If you see anything that suggests misconduct around ballot papers, please contact the AEC on 13 23 26.

The integrity and security of ballot papers is a fundamental value at the AEC.

Australian Government

EIAT
Electoral Integrity Assurance Taskforce

THE REGULATORY ENVIRONMENT

THE ROLE OF THE ACMA IN POLITICAL COMMUNICATIONS

The Australian Communications and Media Authority (ACMA) has a limited role regulating political communications, including communications associated with referendums and local, state and territory or federal elections, and enforces rules in the *Broadcasting Services Act 1992* about the presentation of political and election matter on television and radio.

- Information on the rules around the sending of political messages is available on the ACMA website
- All telemarketing and research calls, including research or opinion polling by or on behalf of political parties, must still comply with minimum standards. You can find out more about these rules on the Do Not Call Register website.

If you think a political call or message has potentially breached these rules you can submit a complaint.

POLITICAL ADS AND 'BLACKOUT' PERIODS

There are rules for election, referendum and political ads on TV and radio.

Information about these rules and how to comply can be found on the ACMA website. This includes:

- advice on election blackout periods, during which election ads cannot be broadcast on TV or radio,
- guidelines regarding the broadcast of political matter.

If you think a political advertisement has potentially breached these rules you can make a complaint via the ACMA website.

ELECTORAL OFFENCES

- There are a number of electoral offences outlined in the *Commonwealth Electoral Act 1918*, some of which are included in Appendix 1 of the AEC's Candidate Handbook .
- Depending on the circumstances, relevant State and Territory offences may also apply.
- For offences that may be classified as electoral fraud, reports can also be made to the AEC. More information about electoral fraud is available on the AEC website

Reporting fraud to the AEC:

- Call 1300 795 898
- Via the website
- By email to fraud@aec.gov.au

THE LOBBYING CODE OF CONDUCT

If you are a currently working as a third-party lobbyist, or otherwise conducting activities to influence Commonwealth Government decision-making on behalf of a third party, the requirements of the Commonwealth Lobbying Code of Conduct may be relevant to you as a candidate in a Commonwealth election.

Section 12(d) of the Lobbying Code requires a lobbyist or a person listed on the Register of Lobbyists to keep any lobbying activities strictly separate from any personal activities or involvement they may have with a political party. This may include activities you undertake as a candidate.

If you are elected and become a Minister, the Lobbying Code will impose further obligations on you and your staff. We encourage you to familiarise yourself with the obligations for government representatives under the Code.

You should carefully manage any actual or perceived conflicts of interest between your work as a lobbyist and your candidature.

DEFAMATION

The AEC is an independent electoral regulatory body that does not regulate or pursue defamation cases on behalf of candidates or anyone else. This is a personal civil action for you. You should seek independent legal advice about any right of action you may have if you have been subjected to defamatory publication.

What is defamation?

Defamation is the publication of material to one or more people which defames a person or harms their reputation. The person could be named directly or referred to indirectly.

There may be defences available to defamation claims such as:

- the publication was substantially true,
- the person who published the material was offering their honest opinion rather than making a statement of fact, or
- the person innocently distributed the defamatory material.

Note: there are limitation periods which apply to the commencement of these proceedings. The limitation period for an action will be dependent upon the State or Territory in which the action occurred.

Australian Government

EIAT
Electoral Integrity
Assurance Taskforce

LINK DIRECTORY

Important contact details

www.aec.gov.au

info@aec.gov.au

https://www.acma.gov.au/

www.acma.gov.au/complain-about-ads-tv-or-radio#complain-to-us

www.esafety.gov.au

www.esafety.gov.au/report

www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/national-security-hotline

hotline@nationalsecurity.gov.au

https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/user-education/security-tips-social-media-and-messaging-apps

www.cyber.gov.au/report-and-recover

Disinformation and related terms

www.acma.gov.au/online-misinformation

www.acma.gov.au/online-misinformation-and-news-quality-australia-position-paper-guide-code-development

www.aec.gov.au/media/disinformation-register.htm

www.eeas.Europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

www.cyber.gov.au/threats/types-threats/phishing

Trusted electoral information and where to find it

www.aec.gov.au/media/disinformation-tactics.htm
https://www.aec.gov.au/Elections/electoral-advertising/stopandconsider.htm
https://www.facebook.com/AusElectoralCom
https://www.instagram.com/AusElectoralCom/
https://www.threads.net/@auselectoralcom
https://www.youtube.com/AECTV
https://x.com/AusElectoralCom
https://www.tiktok.com/@auselectoralcom
https://formupload.aec.gov.au/Form?FormId=complaint
www.esafety.gov.au/report

Online platforms escalation

https://transparency.meta.com/en-gb/oversight/appealing-to-oversight-board
https://help.Instagram.com/675885993348720
https://support.google.com/youtube/answer/2802027?hl=en&co=GENIE.Platform%3DiOS&oco=1#zippy=%2Creport-a-comment
https://help.x.com/en/rules-and-policies/x-report-violation
https://support.tiktok.com/en/safety-hc/report-a-problem
www.facebook.com/government-nonprofits/best-practices/candidate/
https://www.esafety.gov.au/report

Reporting and accessing support for adult cyber abuse

www.esafety.gov.au/key-topics/adult-cyber-abuse

www.esafety.gov.au/educators/community-education/social-media-self-defence

Protecting yourself online

https://www.cyber.gov.au/protect-yourself

https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-update-your-device-and-software

https://www.cyber.gov.au/protect-yourself/securing-your-accounts/multi-factor-authentication

https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases

https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-back-up-your-files-and-devices

https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/security-tips-personal-devices

https://www.cyber.gov.au/protect-yourself/staying-secure-online/connecting-others-online/secure-your-social-media

Reporting cyber incidents

http://www.cyber.gov.au/

Australian Government | EIAT Electoral Integrity Assurance Taskforce

How you might be targeted

www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/defining-foreign-interference

https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/potential-signs-foreign-interference

https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/institutions-of-democracy

How to protect yourself

https://www.aec.gov.au/Elections/candidates/

Reporting suspected foreign interference

https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

protocol.branch@dfat.gov.au

Foreign Influence Transparency Scheme

https://transparency.ag.gov.au/myregistration

https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme

Personal safety

https://www.police.qld.gov.au/safety-and-preventing-crime/personal-safety

https://www.police.nsw.gov.au/safety_and_prevention/crime_prevention/personal_safety

https://www.police.sa.gov.au/your-safety/crime-prevention-and-security/safety-and-security-tips

https://www.police.wa.gov.au/Your-Safety

https://www.police.vic.gov.au/your-safety

https://www.police.tas.gov.au/services-online/pamphlets-publications/personal-safety-handbook/

https://pfes.nt.gov.au/emergency-service/public-safety-advice/your-emergency-planning/personal-safety

https://www.police.act.gov.au/sites/default/files/PDF/home-and-personal-safety-guide.pdf

https://forms.afp.gov.au/online_forms/report-commonwealth-crime

https://www.afp.gov.au/crimes/crimes-against-commonwealth-australia#:~:text=Report%20a%20crime%20or%20concern.%20We%20can%20investigate%20Commonwealth%20crimes

https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/national-security-hotline

The role of the ACMA in political communications

https://www.acma.gov.au/what-we-do

https://www.acma.gov.au/political-calls-emails-and-text-messages

https://www.donotcall.gov.au/consumers/lodge-a-complaint/

Political ads and 'blackout' periods

https://www.acma.gov.au/election-referendum-and-political-ads

https://www.acma.gov.au/election-and-referendum-blackout-periods

https://www.acma.gov.au/publications/2019-08/guide/guidelines-broadcast-political-matter

https://www.acma.gov.au/complain-about-ads-tv-or-radio#complain-to-us

Electoral offences

https://www.aec.gov.au/elections/candidates/files/EM401-Candidates-Handbook.pdf

https://www.aec.gov.au/footer/fraud.htm

https://formupload.aec.gov.au/Form?FormId=Fraud

fraud@aec.gov.au

The Lobbying Code of Conduct

https://www.ag.gov.au/integrity/publications/lobbying-code-conduct

https://www.ag.gov.au/integrity/publications/lobbying-code-conduct#principles-of-engagement-with-government-representatives