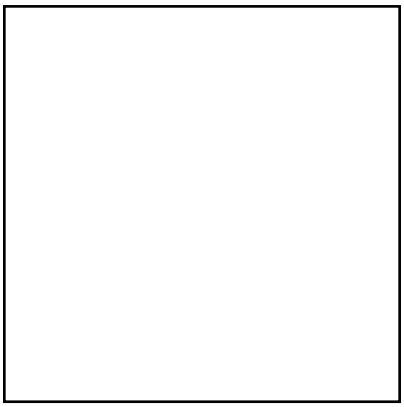

Protect our democratic institutions from foreseeable cyber threats

The problem

Australia is not prepared for cyber attacks or cyber-enabled interference against our democratic institutions. Australia's non-profits, political parties and media organisations are victimised by both cyber criminal and nation-state actors, but often lack the resources and information to build cyber resilience.

Our critical democratic infrastructure includes civil society entities, the media, as well as public bodies including electoral commissions, courts and tribunals, parliaments and national institutions such as the National Archives.

Solutions

Immediate term (2023)

- **The government should publicly signal the criticality – and cyber vulnerability – of democratic institutions, and release targeted cyber uplift guidance.** For non-government organisations, this could be achieved by expanding the Security of Critical Infrastructure Act. For public organisations, an equivalent measure should be considered.

- **The government should commit to provide additional, targeted funding for democratic institutions' cyber resilience**. For non-government organisations, this could be achieved by expanding existing cyber and foreign interference support programs.

Short term (2024)

- **The government should establish accountability frameworks for democratic institutions to spur action.** For government organisations, accountability measures should be public and regularly reported on. Non-government entities could report to the CISC or an equivalent government agency.

Outcomes

- Awareness and access to information for all democratic institutions about the cyber threats they face.
- Government funding and other support to uplift democratic institutions' cyber resilience.
- Accountability frameworks to drive cyber security across our democratic institutions.