Submission to the Independent Review of the Security of Critical Infrastructure Act 2018

Name: [redacted]
Organisation: Australia Myanmar Institute for Democracy, Human Rights and Peace

Summary

This submission evaluates the effectiveness of the Security of Critical Infrastructure Act 2018 (SOCI Act) while drawing on firsthand community-level evidence of foreign interference targeting diaspora groups in Australia. The SOCI Act has improved national awareness of risks relating to critical infrastructure, but significant gaps remain, particularly in relation to hybrid threats that target vulnerable communities connected indirectly to Australia's security environment.

As documented in my report Threats to the Myanmar Community in Australia by the Myanmar Military Junta (2024), during a meeting with two officers from the Department of Home Affairs on 17 October 2024 regarding the Countering Foreign Interference and Countering Foreign Interference Communities Agency, I highlighted that the Myanmar military regime has deployed informants, infiltrators, disinformation agents, and intimidation tactics within the Australian Myanmar diaspora. These activities constitute a form of transnational repression that the current SOCI framework does not adequately address.

While the Act functions effectively for large infrastructure operators, it does not extend sufficient protections, guidance, or support to civil-society organisations or diaspora communities who are often targeted by foreign actors seeking influence or intelligence. This creates unintended vulnerabilities and risks to Australia's social cohesion, information security, and community resilience.

This submission recommends expanding the SOCI framework to better address modern hybrid threats, including foreign interference within diaspora communities, supply-chain vulnerabilities, disinformation, and emerging AI-driven risks.

1. Is the SOCI Act achieving its intended objectives?

The SOCI Act has strengthened national capacity to identify and manage risks relating to espionage, sabotage, and foreign interference across critical infrastructure sectors. It has improved reporting processes and increased the accountability of infrastructure operators.

However, significant gaps remain in addressing **indirect forms of foreign interference**, particularly those targeting diaspora and refugee communities in Australia. As outlined in my report, *Threats to the Myanmar Community in Australia by the Myanmar Military Junta* (2024), the Myanmar military regime actively infiltrates community events, monitors online communications, and intimidates members of the Australian Myanmar diaspora. These activities represent foreign interference that affects social resilience, civic participation, and trust — yet they are not fully captured by SOCI protections.

Therefore, while the Act achieves many of its core objectives, it falls short in addressing broader contemporary national-security challenges, especially hybrid threats that exploit vulnerable communities.

2. Is the SOCI Act functioning as intended?

The Act is functioning effectively within its current scope. Major infrastructure operators generally understand their obligations and work closely with the Australian Government to comply with risk-management requirements.

However, the scope of the Act may be too narrow to respond to the full spectrum of foreign interference tactics now present in Australia. The Myanmar military junta's surveillance, infiltration, and disinformation targeting diaspora communities demonstrate how foreign actors exploit sectors outside formal "critical infrastructure" to influence, destabilise, or gather intelligence. These activities are documented in my 2024 report and include monitoring protests, collecting personal data, and intimidating activists through threats to family members overseas.

Because community organisations, multicultural associations, and grassroots networks fall outside the SOCI framework, foreign interference can occur unchecked. As a result, the Act functions as intended but does not yet provide a whole-of-society approach suited to modern threat environments.

3. Is the SOCI Act causing any unintended consequences?

One unintended consequence is that heightened regulation of large operators creates a **perception of uneven protection**, where smaller organisations — including diaspora-based community groups that face real foreign-interference risks — receive limited support or security guidance.

Without clear frameworks for community-level protection, diaspora groups may feel forced to self-police or view newcomers with suspicion. My report documents how disinformation spread by junta-linked agents has already caused division and mistrust within the Myanmar community in Australia. These dynamics undermine social cohesion, civic participation, and Australia's broader national-security resilience.

Additionally, because the SOCI Act's obligations apply mainly to large operators, community organisations that play key roles in communication, coordination, and settlement support may unintentionally be left vulnerable to foreign interference, information theft, and intimidation.

4. Are there new or emerging threats the SOCI Act cannot currently manage?

Yes. Several emerging threats fall outside the SOCI Act's current capacity:

a) Transnational repression & diaspora targeting: Foreign governments, including the Myanmar military junta, are increasingly targeting diaspora communities through infiltration, coercion, surveillance, and intimidation. These tactics undermine democratic participation and social cohesion but are not yet captured by SOCI obligations.

b) Disinformation campaigns: Diaspora communities are targets of deliberate false-information campaigns aimed at creating division, undermining trust, and influencing public narratives. These information attacks affect resilience but sit outside existing SOCI definitions.

c) Community-infrastructure vulnerabilities: Organisations that provide settlement services, cultural coordination, or community communication often act as de facto infrastructure for vulnerable groups, yet receive no SOCI-related support or guidance.

d) AI-driven threats and cyber-enabled foreign interference: Automated surveillance, deepfakes, and AI-enhanced disinformation pose new risks requiring stronger national coordination beyond traditional infrastructure security.

These emerging threats demonstrate the need to expand SOCI's framework to better protect communities and civil society alongside physical infrastructure.

Conclusion & Recommendations

1. **Expand the SOCI framework** to address hybrid foreign-interference threats targeting diaspora communities.
2. **Provide guidance and support** for community organisations and multicultural groups exposed to foreign monitoring or coercion.
3. **Improve cross-agency coordination** between Home Affairs, intelligence agencies, multicultural services, and community leaders.
4. **Develop policies addressing transnational repression**, including monitoring, intimidation, and disinformation directed at diaspora Australians.
5. **Strengthen information-sharing protections** to safeguard vulnerable communities from reprisals by foreign actors.

About the Author:

[redacted]