Appendix A – Resources

Resources on and guidance against threats to industry, critical infrastructure and academia

- **The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) (www.cyber.gov.au)**
    - The ASD's ACSC is the Australian Government's lead on developing technical cyber security advice and guidance. It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and help make Australia the most secure place to connect online.
    - Through the ASD's ACSC, ASD provides cyber security advice and assistance to Australian governments, businesses, and individuals, as per its established functions under the *Intelligence Services Act 2001.*
    - Visit the ASD's ACSC website for cyber security guidance and programs, including the Strategies to Mitigate Cyber Security Incidents and the Australian Government Information Security Manual.
    - ASD's Annual Cyber Threat Report is the ASD's ASCS's flagship unclassified publication. The annual reports provide an overview of key cyber threats impacting Australia, how the ASD's ACSC is responding to the threat environment, and crucial advice for Australian individuals and organisations to protect themselves online.
- **Australian Signals Directorate's Cyber Security Partnership Program and Australian Signals Directorate's Business Partner (https://www.cyber.gov.au/partnershipprogram)**
    - ASD's Cyber Security Partnership Program enables Australian organisations and individuals to engage with the ASD's ACSC and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy.
    - ASD's Cyber Security Partnership Program is delivered through ASD's network of Partnership Program State/Territory Offices, physically located in Adelaide, Brisbane, Melbourne, Perth, and Sydney, along with outreach services virtually located in Darwin and Hobart.
    - If you do not meet the eligibility to register as an ASD's Cyber Security Partner, but are an Australian business with a valid Australian Business Number, you are eligible to register as an ASD's Business Partner.
    - ASD's Business Partnership is available to Australian entities with a valid ABN and is suitable for organisations who would like to receive the latest information from the ASD's ACSC, but do not meet the eligibility to register as an ASD's Cyber Security Partners.
    - This tier of partnership provides organisations with a better understanding of the cyber security landscape and outlines the steps required to protect themselves from cyber security threats.
    - ASD's Business Partners will receive:
        - a monthly newsletter containing news, publications and advisories produced by the ASD's ACSC for the month prior;
        - a subscription to the ASD's ACSC Alert Service;
        - targeted guidance and relevant information on cyber.gov.au; and
        - invitations to relevant, informative events the ASD's ACSC are presenting/attending.
    - By partnering with the ASD's ACSC, Australian organisations will receive timely information to assist them in keeping their systems and networks secure.

- **Australian Security Intelligence Organisation (ASIO) Outreach (www.asio.gov.au/outreach)**
    - The ASIO Outreach program provides threat and security information to government and industry stakeholders in a variety of ways, including via:
        - a subscriber-controlled website portal;
        - ASIO-hosted briefings;
        - face-to-face engagement with executives and staff; and
        - joint government and industry forums.
    - The ASIO Outreach subscriber portal, as part of ASIO's Outreach program, contains intelligence-backed reporting on the domestic and international security environment, drawn from ASIO's information holdings and expertise—including the multi-agency National Threat Assessment Centre, and ASIO's protective security area (T4).

    To apply, visit the ASIO website.

    - ASIO's protective security advice informs Government, business, and owners of critical infrastructure on current and emerging threats, and the design and application of security policy. This advice aims to build resilience and capability to ensure stakeholders can make fully informed decisions to mitigate security threats and manage risk.
- **Cyber and Infrastructure Security Centre (https://www.cisc.gov.au)**
    - Within the Department of Home Affairs, the Cyber and Infrastructure Security Centre drives an all-hazards critical infrastructure regime in partnership with governments, industry, and the broader community.
    - They actively assist Australian critical infrastructure owners and operators to understand the risk environment and meet their regulatory requirements for the shared benefit of all Australians.
    - The Cyber and Infrastructure Security Centre's Critical Infrastructure Annual Risk Review addresses the dangers posed to Australia's critical infrastructure. It provides a summary of security risks relating to Australia's critical infrastructure.

Resources for geopolitical information, including public attributions and international sanctions

Sanctions

- **Department of Foreign Affairs and Trade's (DFAT) Consolidated List (https://www.dfat.gov.au/international -relations/security/sanctions)**
    - The Consolidated List is a list of all persons and entities listed under Australian sanctions laws. Listed persons and entities are subject to targeted financial sanctions. Listed persons may also be subject to travel bans.
    - The Australian Sanctions Office (ASO) maintains the Consolidated List and updates it regularly. You can subscribe to their email list to receive updates.
- **Department of Foreign Affairs and Trade Guidance notes**
  (Guidance | Australian Government Department of Foreign Affairs and Trade)
    - The ASO is the Australian Government's sanctions regulator. As the sanctions regulator, the ASO:
        - provides guidance to regulated entities, including government agencies, individuals, business and other organisations on Australian sanctions law; and
        - works with individuals, business and other organisations to promote compliance and help prevent breaches of the law

- In addition to providing guidance on specific sanctions frameworks, the ASO provides information on a number of sanctions-related issues that span multiple frameworks or that may affect specific industries.

Cyber attribution and security information

- Search – '(insert country) Australia cyber attribution'

Business risk information

- **United Kingdom (UK) Government's Overseas Business Risk collection (https://www.gov.uk/government/collections/overseas-business-risk)**
  - The UK Government provides country-specific guides for UK businesses on political, economic and security risks when trading overseas.
- **Office of the United States Trade Representative Special 301 Report – Intellectual Property Protection (https://ustr.gov/issue-areas/intellectual-property/special-301)**
  - The "Special 301" Report reflects the outcome of a United States (US) congressionally mandated annual review of the global state of intellectual property (IP) rights protection and enforcement.
  - The review reflects the Administration's resolve to encourage and maintain enabling environments for innovation, including effective IP protection and enforcement, in markets worldwide, which benefit not only US exporters but the domestic IP-intensive industries in those markets as well.
  - The Report identifies a wide range of concerns that limit innovation and investment, including:
    - the deterioration in the effectiveness of IP protection and enforcement and overall market access for persons relying on IP in a number of trading partner markets;
    - reported inadequacies in trade secret protection in countries around the world, as well as an increasing incidence of trade secret misappropriation;
    - troubling "indigenous innovation" policies that may unfairly disadvantage US rights holders in foreign markets;
    - the continuing challenges of copyright piracy and the sale of counterfeit trademarked products on the Internet;
    - additional market access barriers, including non-transparent, discriminatory or otherwise trade-restrictive, measures that appear to impede access to healthcare and copyright-protected content; and
    - ongoing, systemic IP enforcement issues at borders and in many trading partner markets around the world.

Geopolitical Information

- **Australian Strategic Policy Institute (ASPI) (https://www.aspi.org.au/)**
  - ASPI is an independent, non-partisan think tank that provides advice for Australian and global leaders and policy makers.
  - ASPI contributes to public discussion of strategic policy issues in the Indo-Pacific region and is a recognised and authoritative Australian voice in international discussion on strategic, national security, cyber, technology and foreign interference issues.
- **Lowy Institute (https://www.lowyinstitute.org/)**
  - The Lowy Institute is an independent, nonpartisan international policy think tank located in Sydney, Australia. The Lowy Institute conducts policy-relevant research regarding international political, strategic and economic issues from an Australian perspective.

Resources and tools on jurisdictions and politically exposed persons

- **OpenSanctions: Find sanctions targets and persons of interest (https://www.opensanctions.org/)**
    - OpenSanctions is an international database of persons and companies of political, criminal, or economic interest.
    - Their data combines the sanctions lists, databases of politically exposed persons, and other information about persons in the public interest into a single, easy-to-use dataset.
- **World Justice Project Rule of Law Index (https://worldjusticeproject.org/rule-of-law-index/)**
    - The Rule of Law Index evaluates countries and jurisdictions around the world according to a framework that measures constraints on government powers, absence of corruption, open government, fundamental rights, order and security, regulatory enforcement, civil justice, and criminal justice.
- **Attorney-General's Department's Foreign Influence Transparency Scheme Public Register (https://transparency.ag.gov.au/)**
    - The purpose of the scheme is to provide the public with visibility of the nature, level and extent of foreign influence on Australia's government and politics.
    - Individuals or entities are required to register certain activities under the scheme if they are taken on behalf of a foreign government, foreign political organisation, foreign government related entity, or foreign government related individual.
- **Australian Transaction Reports and Analysis Centre (AUSTRAC) information and guidance on politically exposed persons (https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/politically-exposed-persons-peps)**
    - AUSTRAC is Australia's financial intelligence unit and anti-money laundering and counter-terrorism financing (AML/CTF) regulator.
    - AUSTRAC's quick guide on politically exposed person (PEP) provides a brief snapshot to assist companies are meeting their AML/CTF obligations and protecting their business and the community from serious and organised crime.
- **Financial Action Task Force's high-risk and other monitored jurisdictions (https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html) and Politically exposed persons guidance (https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf)**
    - The Financial Action Task Force (FATF), an inter-governmental body that sets AML/CTF standards, monitors the progress of members, and identifies vulnerabilities that could expose the international financial system to misuse. FATF provides regular statements about high-risk or non-cooperative jurisdictions. These jurisdictions have inadequate AML/CTF regimes and have financial systems that are open to criminal abuse.
    - Many countries and organisations hold FATF's PEP guidance as the benchmark test of who may be a PEP.
- **Financial Action Task Force's 'Black and grey' lists (https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html)**
    - The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing in two FATF public documents that are issued three times a year. The FATF's process to publicly list countries with weak AML/CFT regimes has proved effective. As of October 2024, the FATF has reviewed 137 countries and jurisdictions and publicly identified 112 of them. Of these, 85 have since made the necessary reforms to address their AML/CFT weaknesses and have been removed from the process.