Australian Government

Critical Infrastructure Centre

Protecting your critical infrastructure asset from foreign involvement risk

Critical infrastructure operators face a wide range of risks to the continuity of their operations. Most operators have a strong understanding of the vulnerabilities of their assets, and have implemented comprehensive security regimes. However, the national security threats of espionage, sabotage and coercion emerging from increases in foreign involvement, outsourcing, offshoring and supply chain dependencies can create particular national security risks that are not as well understood or managed. Supply chains, including outsourcing and offshoring arrangements, are particularly vulnerable. Critical infrastructure operators should identify and manage foreign involvement risk within their organisation's risk management framework.

The Critical Infrastructure Centre is developing a range of guidance material, in collaboration with critical infrastructure operators, to assist in managing foreign involvement risks. The following six security principles have been modelled on advice provided to government agencies. Industry is invited to comment on the principles and provide any additional feedback on the nature and scope of future guidance material.

1 Protect against insider threat by identifying sensitive job roles and undertaking pre-employment screening using a risk-based approach

Insiders know their employer's vulnerabilities and how to exploit them, and could be recruited to take advantage of their sensitive access. Risk-based employment checks and ongoing monitoring for breaches will decrease the risk of insider threat.

2 Know where your sensitive information or bulk data is stored, who has access to it and how well it is protected

Data stored offshore may be subject to foreign countries' laws, such as collection of sensitive information, which may be incompatible with Australia's legal framework. Determine if your suppliers store your data offshore and ensure you are satisfied with that country's legal framework.

3 Limit access to physical facilities and services to individuals with a genuine and legitimate need

Access to restricted areas or control systems should only be provided to individuals with a need to access for legitimate business purposes.

4 Ensure key technologies, such as industrial control systems, are secure by implementing effective cybersecurity practices

Implementing key cybersecurity measures can prevent the majority of incidents and make it harder for adversaries to compromise your systems or data. Ensuring employee awareness of simple cybersecurity practices will limit opportunities for cyber breaches.

5 Understand and manage risks in outsourced and offshored functions

Insert clauses into supplier contracts requiring notification of changes of ownership, day-to-day operations, and management. Know where your data is stored, where technical support is based, and how breaches are reported, including cybersecurity incidents. Visibility of supplier activities is crucial in securing your supply chain.

6 Embed organisational security culture through governance and by promoting security-conscious behaviour

Promote a strong security culture through training, awareness raising and encouraging reporting of suspicious activity. Establish governance arrangements such as a Chief Security Officer and security committees, and establish contacts to receive reporting and respond to security incidents.

Please see reverse for useful resources that may assist to implement the six principles.

Australian Government | Critical Infrastructure Centre

Guidance and support to better understand and manage foreign involvement risk in critical infrastructure supply chains

A variety of guidance material exists that will assist in implementing these six principles. While many of these documents have been designed primarily for government use, they are highly relevant for protecting businesses and critical infrastructure assets when considered in the context of foreign involvement in your supply chain and differences in business and legal cultures in offshore suppliers.

Critical Infrastructure Centre - www.cicentre.gov.au

- The Centre brings together expertise and capability from across the Government to manage the complex and evolving national security risks from foreign involvement in Australia's critical infrastructure. If you would like to engage with the Centre, please contact us on +61 2 5127 7387 or email enquiries@cicentre.gov.au

Trusted Information Sharing Network (TISN) - www.tisn.gov.au

- A secure platform for business-government information-sharing and initiatives on critical infrastructure resilience. Critical infrastructure owners and operators can seek TISN membership by contacting the Centre.

Australian Security Intelligence Organisation (ASIO) - bglu.asio.gov.au

- **Business and Government Liaison Unit (BGLU)** – the BGLU secure website hosts intelligence-backed reporting, which is drawn from the full range of ASIO's information holdings and experts *(Principles 1-6)*
- **T4 Protective Security** – provides a wide range of practical security advice for security managers on the BGLU website *(Principles 3, 5)*

Protective Security Policy Framework (PSPF) - www.protectivesecurity.gov.au

Provides policy and better practice guidance for protecting people, information and assets. Guidance that may be relevant to critical infrastructure owners and operators includes, but is not limited to:

- **Eligibility and suitability of personnel, and Ongoing assessment of personnel** *(Principle 1)*
- **Security governance for contracted service providers** *(Principles 2, 5)*
- **Access to information, and Entity facilities** *(Principle 3)*
- **Safeguarding information from cyber threats** *(Principle 4)*
- **Management structures** *(Principle 6)*

Australian Cyber Security Centre (including ASD and CERT resources) - www.acsc.gov.au

- **Essential Eight** – baseline cyber strategies to mitigate and prevent cybersecurity incidents *(Principle 4)*
- **Information Security Manual** – guidance in applying risk-based controls and implementing strong information security measures *(Principle 4)*
- **Strategies to Mitigate Cyber Security Incidents** – cyber security guidance addressing targeted intrusions, external adversaries, malicious insiders and industrial control systems *(Principles 1, 4)*
- **Top Control Systems Tips** – simple mitigations that improve security in operational technology environments *(Principle 4)*
- **Remote Access Protocol** – a secure procedure for allowing external party access to critical infrastructure control networks to ensure continuity of service *(Principles 2, 5)*

Austrade - www.austrade.gov.au

- **Anti-bribery & Corruption: A guide for Australians doing business offshore** – practical guidance to help build an organisational culture of compliance to counter risks of corruption offshore *(Principles 1, 6)*

Other resources

- **United States Department of Homeland Security - www.dhs.gov** – offers a wide array of free tools, guidance materials and resources online that can also apply to Australian critical infrastructure *(Principles 1-6)*
- **National Institute of Standards and Technology Cybersecurity Framework - www.nist.gov** – voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organisations to better manage and reduce cybersecurity risk *(Principle 2)*
- **United Kingdom Centre for the Protection of National Infrastructure (CPNI) - www.cpni.gov.uk** – advice and resources about reducing insider risk, optimising people in security and disrupting hostile reconnaissance in critical infrastructure *(Principles 1-6)*