Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Factsheet for Critical Infrastructure

Data Storage, Access and Control

February 2025

Australia's critical infrastructure increasingly relies on cloud service providers (CSPs) and co-location data centres to store and process business critical data. Regardless of whether data is stored in Australia or overseas, access and security controls, and understanding of foreign ownership, control or influence, can help reduce national security risks.

The storage, transmission or processing of sensitive operational information inside and outside Australia, poses a material risk as identified in the *Security of Critical Infrastructure Act 2018* (SOCI) Risk Management Program Rules. This factsheet assists responsible entities under SOCI to mitigate these risks.

What are data access and control risks?

As data becomes more dispersed it becomes increasingly vulnerable to compromise. Threats such as espionage, sabotage and foreign interference may emerge when a foreign entity has the power to control or influence an entity, referred to as FOCI (foreign ownership, control and influence) risks.

Outsourcing, offshoring and supply chain dependencies can increase FOCI risks. In an increasingly complex and challenging strategic environment, FOCI risks can impact the confidentiality, availability and integrity of data, for example:

Foreign Disclosure Laws

Some foreign governments mandate access to privately held information in data centres located within their jurisdiction. Consequently, foreign-owned or operated data storage facilities may be legally compelled to provide other governments with access to client data without the client's knowledge or consent.

Some foreign laws apply to the entirety of a company's infrastructure, regardless of geographic location of an asset or jurisdiction.

Foreign Direct Investment

If a data centre is subject to foreign direct investment (FDI), shareholders may gain greater influence or control over security related decisions. In some cases, foreign investors could gain access to data. When these shareholders have interests contrary to Australia's, there is an increased risk to data security. Shareholders may maintain close links with government officials or be pressured by a government to undertake acts contrary to Australia's interests. An inability to monitor, regulate offshore data centres in some countries is a risk associated with offshore data storage.

Physical security and natural hazards

It may be impractical for an entity to audit foreign data storage procedures for compliance with various Australian legislation, such as the *Privacy Act 1988*. This could limit transparency.

Commercial and reputational considerations

In addition to the national security risks outlined above, the commercial risks to businesses in the event of data compromise, are many. Large scale data breaches could lead to significant financial losses which could be compounded by reputational damage.

CONTACT US | enquiries@CISC.gov.au | CISC.gov.au

In addition to safeguarding data, keeping storage or processing components secure can future proof businesses in the face of rapidly growing demand for trusted and secure data storage by Australia's critical infrastructure

What can be done to mitigate these risks?

Entities can take a number of actions to mitigate risks associated with data storage, access and control. The Australian Cyber Security Centre (ACSC) produces the **Information Security Manual** (ISM), which provides a cyber-security risk framework that organisations can apply to protect their systems and data from cyber threats. The **Infosec Registered Assessors Program** (IRAP) can assist in determining your data storage facilities' compliance with the ISM; however, this may be impracticable for accessing providers in certain jurisdictions.

1. Store data at secure and trusted facility

Storing data in a location where access and security controls are clear and verifiable can mitigate risks to the integrity and availability of data. Consider both the location and FOCI of the chosen facility and the relevant jurisdictions' approach to transparency and the rule of law. Understanding the data collection laws of relevant jurisdictions will help in managing data security risks that may emerge from FOCI.

2. Conduct risk assessments

Businesses should conduct risk assessments in relation to their selected data storage or processing providers. This analysis is particularly pertinent when contracting data storage from a provider that may attract FOCI concerns. Due diligence should include thorough examination of both who controls, and who has invested in the data storage provider.

3. Maintain strong cyber security hygiene

This should be a crucial priority for any business storing data. Implementing key cyber security measures can prevent the majority of incidents and make it harder for adversaries to compromise systems or data.Ensuring employee compliance with cyber security practices will reduce opportunities for low complexity cyber breaches. Proper due diligence, the use of encryption, and the implementation of comprehensive risk assessment frameworks in line with Australian Government advice can assist in mitigating national security threats.

4. Maintain strong visibility

Data storage contracts can be an effective mechanism to maintain data integrity, confidentiality and availability. The ACSC's ISM provides guidance on how contractual security requirements can protect data stored with CSPs.

Common contractual requirements include requiring notification of changes of ownership, day-to-day operations, and management. Businesses should be aware of their cyber supply chain and know where their data is stored, where technical support is based, and how breaches are reported, including cyber security incidents. Contractual clauses can be used to ensure entities are notified, and possibly required to approve any changes to IT or operational technology (OT) networks or security systems. These clauses can apply to changes in hardware, to changes in security policies and procedures, and to the use of subcontractors. These clauses reduce the likelihood that changes of ownership will weaken the security posture of an offshore data centre. It is critical to ensure contracts include effective mechanisms to ensure compliance with contractual obligations. For further information regarding supply chain risks refer to **ACSC's guidance**.

What other resources exist?

The Department of Home Affairs manages the assessment and certification of data centres and cloud service providers that host sensitive and classified Australian Government data under the **Hosting Certification Framework** (HCF). The **Protective Security Policy Framework** (PSPF) Policy 11 articulates that Government entities must ensure the secure hosting of sensitive and classified government information and data through the use of certified services and associated infrastructure by applying the HCF. Facilities that are HCF certified have been formally assessed and successfully met the requirements associated with storing Government data.

Entities responsible for critical infrastructure who are also members of the Defence Industry Security Program (DISP) should refer to the **Defence Security Principles Framework** (DSPF), specifically Principle 10 – *Assessing and Protecting Official Information* and Principle 23 – *ICT Certification and Accreditation*.

Where can I find out more?

Within the Department of Home Affairs, the CISC drives an all hazards critical infrastructure risk management regime in partnership with government, industry and the broader community. The CISC assists critical infrastructure owners and operators to understand the risk environment and meet their regulatory obligations. More information can be found on the CISC website. Further information on what the Australian Government is doing to build Australia's cyber resilience can be found in the 2023-2030 Australian Cyber Security Strategy.