Australian Government
Department of Home Affairs

Factsheet - Technology Vendor Review Framework

On 20 December 2024 the Minister for Home Affairs announced the finalisation of Australia's Technology Vendor Review Framework (the framework). The framework is a key measure under the *2023-2030 Australian Cyber Security Strategy*.

This factsheet provides the Australian public and industry with information on the framework's purpose, scope and function.

Key Points

- The framework establishes the Australian Government's dedicated and proactive process to consider foreign ownership, control or influence (FOCI) risks associated with technology vendors.
- With the framework, the Australian Government is in a strong position to analyse and provide guidance on technology vendor risks to inform public and private sector procurement decisions about the security of technology products and services.
- The framework does not introduce any new legislative authorities or regulation. It provides a robust, comprehensive, consistent and risk-based approach for the Government to understand vendor risks and develop appropriate mitigations.
- Consultation will be a key feature of reviews under the framework. The Australian Government will be engaging directly with organisations and end-users, as appropriate, to understand the risks introduced by a product or service, and the availability of mitigations.
- The framework will not be released publicly to ensure the integrity of the framework's processes and protect information relating to national security.

Overview

Australia is a net technology importer – our economy relies on the availability of overseas technology products and services. Foreign technology companies offer significant value, capabilities and opportunities for the Australian economy and society. They are essential for Australia's long-term economic security, stability and prosperity, including Australia's net zero transition. Recognising the adoption of new and emerging technologies is a key driver of economic growth and prosperity, the Australian Government is committed to ensuring that Australia remains an open, safe and attractive place to do business.

Foreign owned, controlled or influenced vendors supply and operate a vast range of technology products and services in Australia. The majority of these vendors do not present a threat to Australia's interests. However, in some cases, the application, market prevalence or nature of certain technologies, coupled with foreign influence, could present unacceptable risks to parts of the Australian economy. This is particularly true if the vendor is owned, controlled or influenced by foreign governments with interests which conflict with Australia's. By introducing the framework, the Australian Government will proactively assess the risks of technology vendors and consider mitigations where these risks are unacceptable.

The Government has not established the framework to ban or restrict vendor access within the Australian economy, or target vendors from specific nations. The framework will ensure the Australian Government fully understands the risks presented by technology vendors, to inform proportionate and consistent risk mitigations. The framework is founded on a risk-based approach, ensuring outcomes do not discourage technology adoption.

The framework complements existing policies and legislation, including the Protective Security Policy Framework and the *Security of Critical Infrastructure Act 2018*.

What is foreign ownership, control, or influence?

If a technology vendor is owned, controlled or influenced by a foreign government, they could be compelled to act against Australia's interests. FOCI can occur through direct ownership, foreign domestic laws, or outside influence (such as political party membership).

Vendors subject to FOCI can be directed to act against Australia's and their own business interests:

- Vendors that access or control sensitive systems and information in Australia are an attractive target to be exploited by foreign governments.
- Vendors could be directed by a foreign government to conduct interference, espionage or sabotage activities in Australia.
- Vendors could be compelled to participate in activities that undermine the security and integrity of systems that Australian organisations and individuals depend on.
- Vendors could be compelled to introduce vulnerabilities into organisational systems, enabling potential data breaches, disruption of services, or sabotage.

What is the Technology Vendor Review Framework?

The framework provides the Australian Government with a dedicated and proactive blueprint to conduct reviews into FOCI vendors and classes of technology.

The framework sets out the process, principles, roles, responsibilities and definitions that empower the Australian Government to identify and centrally review technology vendor-related FOCI and correlating security risks across government, critical infrastructure and the broader economy.

The framework will strengthen the Australian Government's understanding of the risks presented by FOCI technology vendors, products and services. This allows mitigations to be considered, designed and applied proportionate to the risks.

In developing the framework, the Australian Government has:

- created the definitions, thresholds, criteria and principles to inform review parameters;
- defined nomination and review processes; and
- established new governance arrangements and lines of accountability, including decision making pathways.

To ensure the integrity of the framework's processes and protect information relating to national security, the framework is not a public document and any reviews undertaken are not intended for public release.

Some review findings will inform future government policies. By identifying emerging risks and vulnerabilities, government can implement mitigations proactively. This ensures that government policies remain robust and responsive to the evolving technological landscape, appropriately balancing security concerns with economic imperatives.

Additionally, other findings may lead to the development of technical guidance aimed at supporting organisations in mitigating identified risks. This guidance may include best practices identified during the review process to help organisations enhance their security.

Review processes

Reviews under the framework will be led by the Department of Home Affairs, in close consultation with relevant Australian Government agencies. Reviews will include the development of market analysis, assessment of national security risks associated with particular technologies and technology vendors, and consideration of risk mitigations. Where appropriate, consultation with relevant technology end users and technology vendors may be undertaken.

The methods and processes for consultation under the framework will vary case-to-case and will depend on the scope of the review, the risks that are identified, and the nature of the mitigations being explored.

The framework and associated governance arrangements provide a process for prioritising assessments based on preliminary risk analysis. Reviews will be targeted and risk-informed, with subjects determined by an initial risk analysis of the product or service. Risk factors include where the product or service is deployed (e.g. government or critical infrastructure), the prevalence and permeation of the product or service, and its nature (e.g. privileged access to sensitive systems or collection of large volumes of sensitive data).

Where can I find more information on managing technology risks?

The Australian Government has developed a range of products to support organisations to consider risks when undertaking procurements, this includes:

- the Australian Signals Directorate's *Identifying Cyber Supply Chain Risk guidance*;
- the Australian Signals Directorate's *Choosing Secure and Verifiable Technologies;* and
- the Department of Home Affairs' *Critical Technology Supply Chain Principles.*