Appendix B – Vendor review questionnaire template

Note: This questionnaire should not take more than 60-90 minutes to complete. While completing the questionnaire, consider whether the information required is available online. You may find some of the information from an internet search, and you can also engage through professional business risk intelligence and advisory groups to help you. Consideration should be given to the confidence level of each of your responses to the questionnaire when weighing your preliminary FOCI assessment. A list of useful resources has been provided in **Appendix A** and throughout the guidance document. An example of a completed questionnaire is available after the template below.

Vendor Name:		
Section 1 - Intent	**Assessment**	**Circle Yes/No**
The beneficial owner of the vendor is from a Five Eyes country (Australia, Canada, New Zealand, UK, and US).		**YES / NO**
*If **YES**, consider cyber security hygiene risks posed by the vendor (see the Australian Signals Directorate's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks"). If **NO**, go to Section 2.*		
Section 2 – Vendor Jurisdiction Hazard	**Assessment**	**Circle Yes/No**
The beneficial owner of the vendor can reasonably be inferred to be controlled from a jurisdiction where there is a risk of a foreign government compelling the vendor to provide access to its private data to the government or its national security agencies (indicated by policies, legal frameworks, or public reports).		**YES / NO**

The beneficial owner of the vendor can reasonably be inferred to be controlled from a jurisdiction that has been the subject of an Australian Government cyber attribution, or the Government has sanctioned the jurisdiction, or an entity within the jurisdiction, under Australian sanction law.		**YES / NO**
The beneficial owner of the vendor can be reasonably inferred to be controlled from a jurisdiction where there is information indicating the use of economic coercion, intellectual property theft and/or technology transfer campaigns targeting Australia and/or a Five Eyes country (Australia, Canada, New Zealand, UK, and US).		**YES / NO**
The beneficial owner of the vendor can reasonably be inferred to be controlled from a jurisdiction where there is information indicating the vendor and/or its parent company has been sanctioned on grounds of corrupt, coercive, collusive or obstructive practices, or other integrity violations in another jurisdiction.		**YES / NO**

*If the answer is **YES** to any of the above, go to Section 4. If **NO**, go to section 3.*

Section 3 – State Ownership, Control or Influence	**Assessment**	**Circle Yes/No**
The vendor is subject to state ownership or control structures, including public information (such as information on securities websites, annual reports and business news reporting) on state shareholding of >50% or outsized state influence in corporate decision-making.		**YES / NO**
There are politically exposed persons (PEPs) in senior leadership roles.		**YES / NO**
There is a special relationship between the vendor and a foreign government, providing a benefit such as special legal rights or legal status in their jurisdiction, or a privilege like unusual state funding arrangements or contracts.		**YES / NO**

*If the answer is **YES** to any of the above, go to Section 4. If **NO**, consider cyber security hygiene risks posed by the vendor (see the Australian Signals Directorate's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks").*

Section 4 – Access and Control	Assessment	Circle Yes/No
The product or service is connected, intermittently or continuously, to the internet, organisation systems or otherwise subject to third-party access.		**YES / NO**
The vendor has excessive or unusual data collection practices or there are indicators the vendor is sharing its data with a foreign military organisation or intelligence/security service (such as through military-civilian industrial cooperation arrangements).		**YES / NO**

*If the answer is **YES** to any of the above, **conduct a vendor FOCI risk assessment**. If **NO**, consider cyber security hygiene risks posed by the vendor (see the Australian Signals Directorate's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks") and risks associated with disruption or suspension of service.*

Preliminary Assessment: