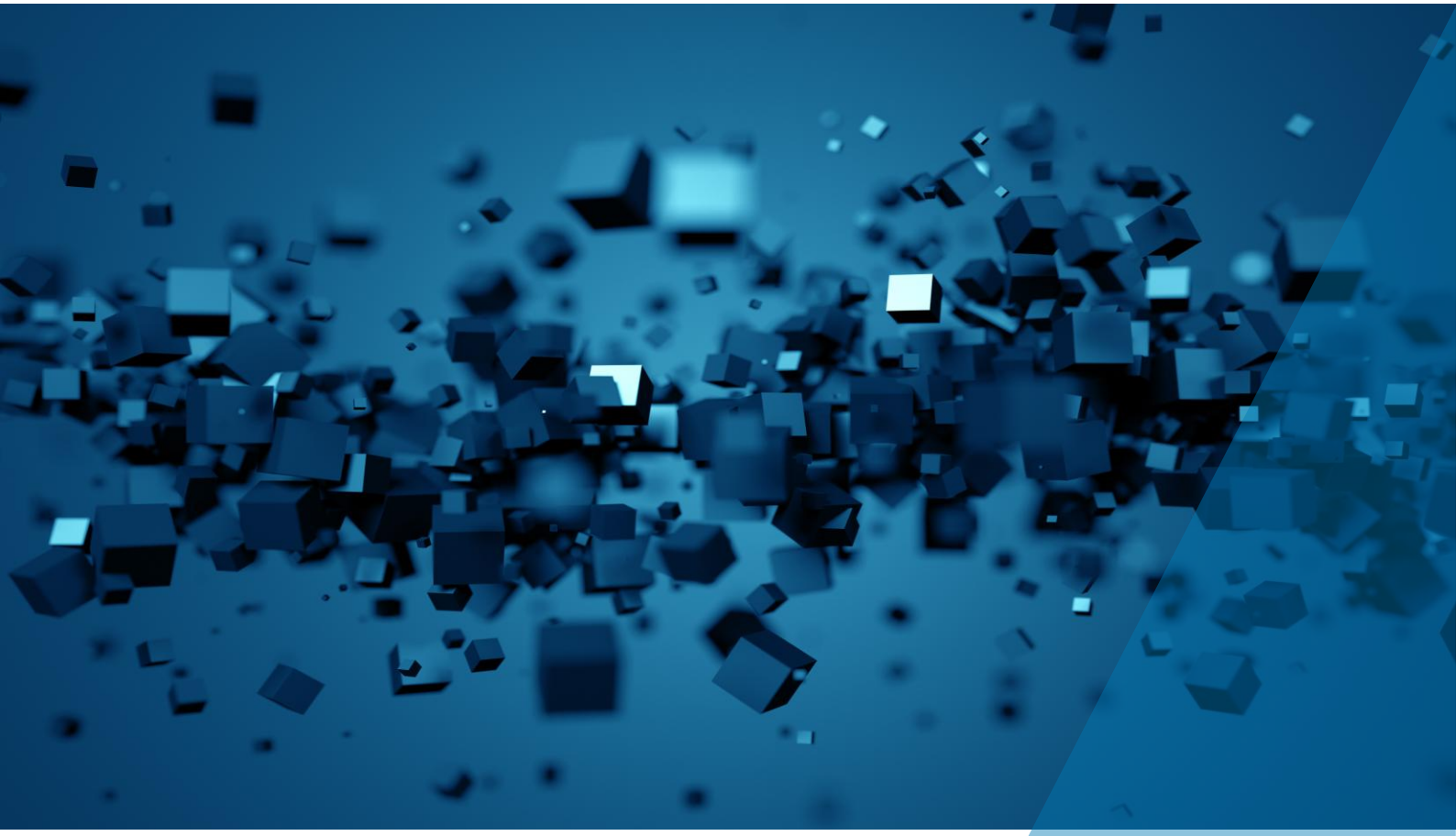
Australian Government
Department of Home Affairs



Foreign Ownership, Control or Influence (FOCI) model clauses for Australian Government entities

Version 1

OFFICIAL

Contact us
Enquiries regarding the licence and any use of this document are welcome at:

Technology Security Policy Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

OFFICIAL

Table of contents

OFFICIAL

Overview

These model clauses are to assist Australian Government entities (Customers) to manage and mitigate foreign ownership, control or influence (FOCI) risks in procurement.

The model clauses:

- are designed to support a range of procurement activities, including tendering, contracting and contract management
- can be used for a range of procurements
- are all optional – Customers should select the relevant clauses that they wish to include in their procurement documents based on FOCI risk for that particular project, and
- use the terminology and format of the Commonwealth Contracting Suite (CCS) documentation so that they can be incorporated into CCS procurement documents.

FOCI risk refers to the ability for vendors to be directed by a foreign government either through direct ownership channels, domestic laws of the foreign jurisdiction, or outside influence.

Procuring technology vendors subject to FOCI increases the risk of exposure to undue influence or acts that can undermine your organisation's security. It could also affect Australia's national interests.

Vendors subject to FOCI can be directed to act against their own business interests. They could be compelled by a foreign government to conduct malicious acts such as undermining the security of their products and services or providing privileged access to systems and client data. Such influence, if not properly managed, can lead to unauthorised access to sensitive information or negatively impact performance and contracts. Managing FOCI risk extends beyond national security; it encompasses protecting your organisation's reputation, your organisation's systems and intellectual property, your business interests, and the privacy of your staff and customers.

Using these model clauses

Customers should consider FOCI risk and security implications when making procurement and contracting decisions. The Department of Home Affairs has published Foreign Ownership, Control or Influence Risk Assessment Guidance to assist with identification of foreign ownership, control or influence risk. Customers should do their own risk assessment for each contract and, if needed, get legal or other advice to determine what types and levels of protection are required in their contract.

Customers should review and amend their contracts to ensure consistency between clauses and avoid repetition when incorporating these clauses. In particular, customers may need to clarify that particular clauses are Special Conditions that replace a General Condition. Terminology in these clauses should also be tailored to be consistent with the relevant contract.

Finally, these clauses assume the Customer is a Commonwealth entity and the relevant procurement is occurring in a Commonwealth contracting context.

Relationship with other Commonwealth model clauses

Where FOCI risk is present for a technology related procurement, Customers should consider whether any of the DTA's Cyber Risk Model Clauses (published on BuyICT) should also be included in their Contracts. This is because the development of robust contractual frameworks that adequately mitigate or avoid FOCI risk may be supported by including provisions relating to cyber risk and security issues. Such clauses may be selected and used to:

- ensure data is hosted in a secure and approved location
- govern the use of AI
- protect the security of supply chains
- establish effective audit obligations to support the Commonwealth's ability to verify compliance with the contract and investigate potential breaches, and

OFFICIAL

- require Suppliers to procure cyber risk insurance against particular cyber security risks.

Other Commonwealth-published clause banks may also contain relevant and useful example clauses to support the development of comprehensive and cohesive FOCI clauses for a Contract.

Note: *This document is not legal advice. Drafting notes included in this document are provided as general guidance only. The following clauses are example clauses only. Each is optional. Customers are responsible for using suitable clauses in their Contract*.

OFFICIAL

Approach to Market Model Clause Definitions

Note: *These terms are designed to work with Commonwealth Contracting Suite (CCS) terms. The following definitions can be inserted in the appropriate section of the Approach to Market documentation.*

Standard contract terms such as 'Tenderer', 'Contract', 'Goods and Services', and 'Customer' are not defined in this section. Customers should ensure all defined terms in their Approach to Market documentation are supported with an appropriate definition.

Term	Definition
Beneficial Owner	means an individual or persons who ultimately own or Control an interest in a legal entity or arrangement, including companies, trusts and foundations. Ownership and control may be direct (such as through shares) or indirect (such as shares held by a Third Party on the individual's behalf).
Control	has the meaning given under section 50AA of the *Corporations Act 2001* (Cth).
Consolidated List	means the list of individuals and entities listed in the consolidated sanctions list published by the Department of Foreign Affairs and Trade.
Government Entities	means any non-Australian: a) department of state; b) parliamentary body; c) organ of the state (including the military and judiciary); d) body corporate that is established and prescribed by Law to be a government entity; or e) body corporate that a government other than Australia Controls.
Key Investors and Decision-Makers	means in relation to the Tenderer: a) any person or entity holding, directly or indirectly, more than 20% of the issued share capital or voting rights in the Tenderer (including any majority shareholder); b) any shareholder or group of shareholders acting in concert who has the capacity to exercise meaningful control or influence over the management or strategic direction of the Tenderer; c) any member of the board of directors (or equivalent governing body) of the Tenderer; and d) any person who has, or will have, authority, control or material influence in relation to the decision-making, management and operations of the Tenderer.
Key Personnel	means any Personnel approved by the Customer to provide the Goods and Services to the Customer. **Note:** *Provisions relating to 'Key Personnel' can be altered to refer to 'Personnel' (and vice versa) as is most appropriate in the relevant circumstances.*

OFFICIAL

Term	Definition
Law	means any: a) statute, regulation, rule, by-law, order, ordinance, proclamation, enactment, statutory instrument, binding licence condition or delegated or subordinated legislation that applies or is in operation in the jurisdiction of the Tenderer's incorporation; or b) standard, requirement or condition imposed by a Government Entity.
Material	means any thing in relation to which intellectual property rights arise.
Official Information	means any information: a) developed; b) received; or c) collected, by or on behalf of the Customer to which the Tenderer gains access under or in connection with a Contract, and includes any Material contained in Goods and Services and the terms of a Contract.
Official Resources	includes: a) Official Information; b) people who work for or with the Customer; and c) assets belonging to (even if in the possession of contracted providers) or in the possession of the Customer.
Personnel	means, in relation to the Tenderer, any natural person who is an officer, employee, contracted personnel, labour hire worker, agent or professional adviser of the Tenderer or of a Subcontractor, including any Key Personnel.
Protective Security Directions	means any directions issued by the Secretary of the Department of Home Affairs under the Protective Security Policy Framework.
Protective Security Policy Framework	means the Protective Security Policy Framework available at www.protectivesecurity.gov.au, as amended or replaced from time to time.
Security Incidents	means: a) any actual or suspected breach of security (whether relating to information, personnel, data, logical, physical or system security or otherwise); b) any contact, request or approach from any person seeking unauthorised access to Official Resources; or c) any circumstance that highlights any actual or potential security vulnerability or which identifies a potential threat to security.
Subcontractors	means any person engaged by the Tenderer to provide any part of the Goods and Services under a contract.

OFFICIAL

Term	Definition
Supply Chain	means a network or system of Subcontractors, agents, suppliers or entities: a) in a direct or indirect business relationship (whether within Australia or internationally) with the Tenderer; or b) which contribute directly or indirectly to the supply of the Goods and Services to the Customer, including entities in the network of business entities or individuals performing, providing, producing, handling, storing, transmitting or distributing: c) the Goods and Services; or d) components of the Goods and Services.
Third Party	means any person, organisation or entity other than: a) the Commonwealth; and b) the Tenderer. For the avoidance of doubt, this definition includes entities which are related bodies corporate of (or entities otherwise related to) the Tenderer.

OFFICIAL

Approach to Market Model Clauses

1. Protective Security Policy Framework

1.1. Managing Foreign Ownership, Control or Influence (FOCI) Risks

1.1.1. Foreign interference occurs when activity carried out by, or on behalf of, a foreign power, is coercive, corrupting, deceptive or clandestine, and is contrary to Australia's sovereignty, values and national interests. Foreign ownership, control or influence (FOCI) is an application of foreign interference.

1.1.2. Under the Protective Security Policy Framework, [insert name of agency] is required to identify and mitigate FOCI risks in its contracting arrangements.

1.1.3. Tenderers must complete Attachment [X] (Foreign Ownership, Control or Influence) of Schedule [X] (Tender Response Forms). A Tenderer's responses to Attachment [X] of Schedule [X] will be evaluated as part of the evaluation of the Tenderer's risk profile.

1.1.4. Tenderers should note that the draft contract contains FOCI obligations that will apply under a resultant Contract.

Note: *The Commonwealth Procurement Rules (CPRs) require Customers to treat potential suppliers equitably regardless of ownership or origin. Customers are also required to consider risks and their potential impact when assessing value for money of tenders and when entering contracts (CPR 8.2). Part of this risk assessment may include FOCI risk for tenderers. FOCI risk may be higher for tenderers in certain jurisdictions, in relation to:*

- *exposure to foreign data collection laws;*
- *foreign government access to a Customer's systems; and*
- *a foreign government's ability to influence decisions of a Supplier.*

The above clause is designed to be included in the Customer's approach to market documentation, to provide Tenderers with the policy background for the Customer's obligations to manage FOCI risks in procurement and prompt the provision of information necessary to assess FOCI risk.

Customers should be aware that Tenderer circumstances can change without notice and introduce new FOCI risks during the life of a Contract. Customers should discuss with their internal procurement team prior to contacting procurementagencyadvice@finance.gov.au for advice in such circumstances.

1.2. Tender Response Form Attachment [X]: Foreign Ownership, Control or Influence

Note: *The following are tender response prompts that can be used in tenders. They are designed to assist Customers to collect FOCI-relevant information from Tenderers that may be required to assess FOCI risk.*

OFFICIAL

Note continued: *The following prompts are sample prompts only. Each prompt is optional and may be changed by Customers as needed to address the FOCI risk assessment and the specific circumstances in which FOCI risk arises. Not every prompt will be appropriate or relevant to every procurement. Customers should carefully consider the purpose and suitability of each prompt before including it in their approach to market documentation.*

Customers should consider the responses from tenderers and conduct appropriate screening of the information provided, including jurisdictions, entities and individuals. Screening should include referring to the DFAT Consolidated List for sanctioned individuals or entities. Additional screening may also be conducted using screening tools. These tools can be used to screen for adverse media, sanctions exposure (this would include exposure under other sanction regimes in addition to Australia) and politically exposed persons.

Tenderers should provide full responses.

A. Origin of corporate identity and activity
A1. In which country or countries is the Tenderer registered to pay tax?
A2. In which country is the Tenderer incorporated?
A3. Describe where the Goods and Services will be produced, delivered or performed (as relevant):
B. Ownership and Control
B1. Provide details and evidence of each member of the Tenderer's corporate group, including parent companies (i.e. legal name, relationship to Tenderer, Beneficial Owners, jurisdiction of incorporation and country of tax residency) (if any):
B2. Provide details of Key Investors and Decision-Makers (including citizenship, country of residence and (if a corporate entity), details of incorporation and country of tax residency):
B3. Provide details of the Tenderer's Beneficial Owner/s (including country of incorporation or operation, and the arrangements for oversight and management of the Tenderer):

OFFICIAL

C. Foreign government engagement
C1. Provide details of Tenderer contracts or engagements with non-Australian Government Entities: **Note:** *Drafters may wish to apply a materiality limit to this prompt (e.g., only require information about the Supplier's contracts or engagements with non-Australian Government Entities with a value over a certain threshold). This may be more practical for tenderers who contract with a significant number of non-Australian Government Entities (e.g., software companies). In such cases, additional or alternative constraints on this prompt may be appropriate. This should be determined in accordance with (and in proportion to) the level of FOCI risk for the proposed contract.*
C2. Provide details of any funding or benefits previously provided to the Tenderer by non-Australian Government Entities:
C3. Provide details of any current or planned funding or benefits to be provided to the Tenderer by non-Australian Government Entities:
D. Interference or influence
D1. Provide details of any previous occasion where the Tenderer has been compelled or directed by a Third Party to provide information about its provision of Goods or Services (if any):
D2. Provide details of any previous occasion where there have been attempts by Third Parties or Government Entities to interfere with or influence the Tenderer's performance of a contract, relationship with customers, provision of Goods and Services or ordinary course of business (if any):
D3. Provide details of any non-Australian Laws or other instruments which may require the Tenderer to provide a Third Party with access to [insert agency]'s information, systems or premises, or information or systems used in relation to the Goods and Services (if any):
D4. Provide details of any non-Australian Laws or other instruments which may require the Tenderer to share information about the [insert agency]'s Goods and Services the subject of this tender or the Australian Government that is not publicly available (if any):

OFFICIAL

D5. Provide details of any Laws or other instruments which may require the Tenderer to perform the Contract or interact with the [insert agency] or Australian Government in a manner directed by a Third Party (if any):
D6. Provide details of any Laws or other instruments which may require the Tenderer to appoint Personnel (including Key Personnel) or Key Investors or Decision-Makers as directed by a Third Party:

OFFICIAL

E. Proposed Personnel
E1. Provide details of the proposed [Key Personnel or Personnel] who will perform the Contract on behalf of the Tenderer [(including countries of citizenship and residence)]: **Note:** *These prompts can be applied in relation to Key Personnel or Personnel generally (noting the definition of Personnel is broader than, and includes, Key Personnel). While it may be onerous to require the suggested information from Tenderers in relation to all Personnel, it may nonetheless be required in some circumstances in order to adequately assess FOCI risk.* *Citizenship and country of residence information about Key Personnel or Personnel may be relevant to particularly sensitive, high-risk procurements. In certain cases, it may be appropriate to include operative clauses which govern the flow of contract information within Suppliers. Alternatively, this element of the prompt can be removed if this information is not relevant.*
E2. Describe the background and other security-relevant checks that have been conducted on the proposed [Key Personnel or Personnel] (or that will be conducted if the Tenderer is selected to perform the Contract), including: • whether the background and other security-relevant checks will be conducted by a Third-Party and if so, the name of the Third Party and details of the arrangement between that Third Party and the Tenderer; • what information has been or will be used to screen personnel and who will have access to this information (including within an assisting Third Party, if relevant); and • when background and security checks are conducted, and if they are re-validated.
E3. Provide details of any security clearances the proposed [Key Personnel or Personnel] hold or have held in Australia or another country: E4. Provide details of any proposed [Key Personnel or Personnel] who currently (or during the course of the Contract, will) work for or perform work for non-Australian Government Entities or registered political parties (if any):
E5. Provide details of any proposed [Key Personnel or Personnel] who have previously worked for a non-Australian Government Entity or registered political party (if any):
E6. Provide details of any proposed [Key Personnel or Personnel] who are close family members of or personal or professional associates with: people who work for Government Entities; or people who work for registered political parties.

OFFICIAL

F. Sanctions and government controls
F1. Provide details of whether the Tenderer, any entity within the Tenderers' corporate group, or Personnel of the Tenderer, have been or are: • on the Consolidated List of the Australian Government; or • subject to sanctions imposed by another government or international organisation (e.g. the World Bank or Human Rights Watch).
G. Utilised technology
G1. Provide details of the technology (including any programs, software, apps, AI and key public websites) that will be used to perform a resultant contract, the people and entities that will access the technology, and whether the technology is administered by the Tenderer or a Third Party (e.g. a managed service provider):
H. Subcontractors and Supply Chain
H1. Provide details of the proposed Subcontractors (if any) that will be used to perform the Contract: **Note:** *This prompt is only necessary where the Tenderer may or is proposing to engage Subcontractors.*
H2. Describe the existing (and any proposed, if different to the existing) Supply Chain arrangements that are required to provide the Goods and Services. For example, if the Tenderer is proposing to supply hardware, the Tenderer might describe where the components of the hardware come from.
H3. Provide details of any previous or current inclusion of any proposed Subcontractor on the Australian Government's Consolidated List or on a sanctions list of another government or international organisation:
This Attachment should be duplicated, and responses provided for each Subcontractor. Those responses should be submitted with this Attachment. **Note:** *Customers might wish to require Subcontractors to answer some or all of the prompts listed in this Attachment (for example, if the Customer requires a thorough understanding of a Subcontractor's character and activities). The above prompt should be included where this outcome is desired. However, the Tenderer is responsible for completing and submitting the tendered information.*

OFFICIAL

I. Access to information
I1. Describe the proposed arrangements for collecting and storing information and data related to the Contract (including whether such arrangements meet [agency to insert the required standards]):
I2. Describe the arrangements in place to protect information and systems from unauthorised access (including any limitations of such arrangements):
I3. Provide details of the Tenderer's corporate group network and information sharing practices (e.g. any shared access to ICT networks, visits to Tenderer facilities, corporate group member collaboration with personnel responsible for the Contract):
I4. Provide details of the Tenderer's corporate group ICT network and information segregation practices:
J. Security history
J1. Describe any previous Security Incidents:
J2. Describe any previous or current non-compliance with the Protective Security Policy Framework or Protective Security Directions:
J3. Provide details of any historical, current or proposed use of technologies developed or managed by banned technology vendors under the Protective Security Policy Framework or Protective Security Directions:

OFFICIAL

Procurement Contract Model Clauses

Note: *The model clauses below are grouped thematically, according to the issue they relate to. Within each 'theme', clauses are further divided into 'general risk' and 'high risk' clauses.*

'General risk' *clauses are designed as standard protections. These clauses are suitable for use in all circumstances where FOCI risk is present.*

'High risk' *clauses are designed as targeted, highly protective clauses for use in specific situations where FOCI risk is moderate to high.*

Only relevant clauses should be selected and used.

Customers may seek commercial and legal advice to determine whether these clauses (or similar clauses) are suitable for use in a contract.

2. Ownership and control

2.1. [GENERAL RISK] Assignment and novation

2.1.1. The Supplier must not assign its rights or seek to novate its obligations under this Contract without the prior written consent of the Customer (which the Customer may grant or withhold in its absolute discretion).

2.1.2. The Customer may conduct due diligence on any new entity proposed to be the assignee or novatee of rights or obligations under this Contract and may treat this as a Change of Control under clause 2.2. The Supplier must give all necessary information to the Customer for this purpose.

2.1.3. If the Customer consents to the Supplier assigning its rights or novating its obligations under this Contract, the Supplier must provide the Customer with a completed deed of assignment or novation (as applicable) in the form required by the Customer.

Note: *This clause is designed to prevent Suppliers from circumventing FOCI assessments by transferring rights or obligations to an unvetted entity. This clause provides the Customer with discretion to withhold consent or impose conditions following due diligence on any new entity that is proposed as assignee or novatee.*

If this clause is used, Customers should take particular care to ensure consistency with any existing assignment provisions in their Contracts.

OFFICIAL

2.2. [GENERAL RISK] Change of control

2.2.1. The Supplier must not undergo a Change of Control without seeking the prior written consent of the Customer.

2.2.2. The Supplier must seek the consent of the Customer as soon as possible before any Change of Control is to occur and not later than twenty (20) Business Days before the proposed date of the Change of Control (**Notification Period**).

2.2.3. A notice of a proposed Change of Control given under this clause must include reasonable details of the proposed Change of Control sufficient to permit the Customer to consider whether to consent to the proposed Change of Control, including (but not limited to):

a) details of the proposed transaction which would result in the Change of Control;

b) the ownership interests in the Supplier which would result from the Change of Control; and

c) a risk assessment contemplating the impact of the Change of Control on the provision of Goods and Services to the Customer, and a corresponding plan to mitigate any such risks.

2.2.4. During the Notification Period, the Supplier must promptly provide the Customer all information requested by the Customer about a proposed Change of Control. This may include details about the Supplier's ownership, corporate structure, beneficiaries, and any controlling entities, in each case, before and after the proposed Change of Control. The Notification Period will be extended by the same amount of time taken to respond to a request.

2.2.5. If the Supplier provides the Customer a notice of a proposed Change of Control, the Customer may:

a) consent to the proposed Change of Control;

b) consent to the proposed Change of Control subject to conditions (breach of which will entitle the Customer to terminate this Contract); or

c) terminate this Contract under clause 9.

2.2.6. If the Customer agrees to the Supplier undergoing a Change of Control that would require a novation of the Supplier's rights or obligations under this Contract, the Supplier must provide the Customer with a completed deed of novation in the form required by the Customer.

Note: *This clause allows Customers to assess emerging FOCI risks posed by changes of control before a change of control takes place, and provides a clear right to terminate if a change in control of a Supplier would create unacceptable risk for the Commonwealth.*

If seeking the prior written consent of the Customer to a Change of Control is not an acceptable commercial position to the Supplier, Customers may instead wish to require notification of a Change of Control. Should this be the preferred commercial position, the above clauses will require modification to reflect that Customer consent is not required. In such cases the Customer should retain the right to immediately terminate if the Change of Control is not acceptable to the Customer.

Customers may tailor the default 20 business day notification period depending on a procurement's sensitivity (for example, longer notice may be appropriate for high-risk or particularly sensitive procurements).

Customers should ensure the termination rights in clauses c) and 9 are consistent with existing termination provisions in their Contracts.

OFFICIAL

2.3. [GENERAL RISK] Ownership

2.3.1. The Supplier warrants that ownership and control of the Supplier is as stated in item [X] of the Contract Details, subject to approval of a Change of Control by the Customer under clause 2.2.

2.3.2. The Supplier must notify the Customer of any planned or actual changes to the ownership or control of the Supplier immediately upon the Supplier becoming aware of such changes.

2.3.3. The Supplier will provide all information requested by the Customer regarding the Supplier's ownership structure and control of the Supplier.

Note: *This clause is designed to provide the Customer with visibility of changes to the Supplier's ownership structure and control of the Supplier, to allow oversight over changes that could create exposure to foreign control, direction or influence. This clause may not be relevant for all contracting scenarios (for example, where the Supplier is Commonwealth-owned).*

2.4. [HIGH RISK] Investment and decision-making

2.4.1. The Supplier warrants that the Key Investors and Decision-Makers and the Supplier's Beneficial Owner/s are as stated in the Contract Details.

2.4.2. The Supplier must notify the Customer of any planned or actual changes to the Supplier's Key Investors, Decision-Makers and Beneficial Owner/s, immediately upon the Supplier becoming aware of such changes.

2.4.3. The Supplier will promptly provide all information requested by the Customer regarding the Supplier's Key Investors and Decision-Makers and Beneficial Owner/s.

Note: *This clause extends beyond legal ownership and control to beneficial ownership and key investors and decision-makers who may exercise material influence even in the absence of legal ownership or control.*

This clause may be appropriate where the Contract involves ongoing strategic or operational engagement with the Supplier (for example, managed services, long-term ICT hosting or security vetting providers). Accordingly, this clause may not be necessary in some circumstances (e.g., short-term transactional procurements).

This clause may also be modified to be less onerous. For example, clause 2.4.2 could be modified so that only certain changes are notifiable to the Customer (rather than all changes).

3. External contact and exposure

3.1. [GENERAL RISK] External contact

3.1.1. The Supplier must notify the Customer immediately if any Third Party requests access to any Customer information or Digital Systems.

3.1.2. The Supplier must provide details of such requests to the Customer and follow reasonable Customer directions on responding to such requests.

Note: *This clause is designed to provide Customers with visibility over requests for Third Party access to Commonwealth information or Digital Systems.*

This clause is suitable for all Commonwealth contracts, and critical for all ICT, hosting, managed services and data handling contracts, specifically where the Supplier operates or administers systems with connectivity to Commonwealth networks.

3.2. [GENERAL RISK] Change in Supplier's country of tax residency or jurisdiction of incorporation

3.2.1. The Supplier warrants that its country of tax residency and jurisdiction of incorporation is as stated in the Contract Details.

3.2.2. The Supplier warrants that any parent company's country of tax residency and jurisdiction of incorporation is as stated in the Contract Details.

3.2.3. If there is a change in the Supplier's:

a) country of tax residency; or

b) any parent company's country of tax residency,

the Supplier must notify the Customer at least 10 Business Days before that change is due to occur, and again when that change has occurred.

Note: *This clause is designed to provide the Customer with visibility over jurisdictional shifts that might alter a Supplier's legal exposure (e.g. new data access laws, sanctions regimes and other extraterritorial powers).*

This clause may be suitable where a Supplier or its parent company has global operations or cross-border corporate and tax structuring.

3.3. [HIGH RISK] External influence

3.3.1. The Supplier must notify the Customer immediately upon becoming aware of:

a) any Law; or

b) any other instrument, request or correspondence (whether formal or informal, direct or indirect),

which:

c) compels or attempts to compel the Supplier to:

i. provide a Third Party with access to any Customer information or Digital Systems;

ii. share information about the Customer, this Contract or the Australian Government that is not publicly available; or

iii. perform this Contract or interact with the Customer or Australian Government in a manner directed by a Third Party.

3.3.2. Without limiting clause 3.3.1, the Supplier must notify the Customer immediately upon becoming aware of any:

a) interference with or influence of; or

OFFICIAL

b) attempts to interfere with or influence,

the Supplier's performance of this Contract or relationship with the Customer or Australian government.

> **Note:** *This clause is designed to provide the Customer with visibility over pressure that may elicit disclosure of Commonwealth information by the Supplier, shape performance of the Supplier or influence the Supplier's interactions with the Commonwealth.*
>
> *This clause may be suitable where Suppliers operate in or are exposed to foreign legal jurisdictions (including through parent and other affiliate locations and entities). However, noting that Suppliers are likely to be bound by various obligations not to disclose information (see, for example, clause 8.3 below), this clause could be reserved for high FOCI risk situations.*

3.4. [HIGH RISK] Contracts with Government Entities

3.4.1. The Supplier warrants that its contracts and other engagements with Government Entities (other than Australian Government Entities) are as advised by the Supplier to the Customer prior to the execution of this Contract.

3.4.2. The Supplier must immediately notify the Customer upon the earliest of:

a) bidding for;

b) entering into; or

c) being approached in relation to,

additional contractual relationships or engagements with non-Australian Government Entities.

> **Note:** *This clause is designed to provide the Customer with visibility over the Supplier's engagements with foreign Government Entities that might create information sharing gateways, operational dependencies or conflicting obligations to the Supplier's obligations in Commonwealth contracts.*
>
> *This clause may be suitable where a Supplier operates internationally or is subject to political, regulatory or contractual leverage from foreign governments or state-linked enterprises. However, Suppliers which routinely contract to other governments may not accept this clause on the basis that it is not (for example) practicable or permissible under the terms of other contractual arrangements to issue the notifications required under this clause. Nonetheless, Customers may wish to request that this clause is included to protect Commonwealth interests in high-risk scenarios where (for example) the Commonwealth wishes to understand potential threats to its supply in a competitive market or where provision of the same or similar Goods and Services to another government is unacceptable or undesirable.*

OFFICIAL

4. Sanctions

4.1. [GENERAL RISK] No sanctions

4.1.1. The Supplier warrants that it is not on the Commonwealth's Consolidated List of individuals and entities to which Australian Sanctions apply and none of its Key Personnel or Subcontractors are on, or are a member of an entity on, that list.

4.1.2. The Supplier warrants that neither it, nor any member of its corporate family, has been subject to any Sanctions on the basis of corrupt, coercive, collusive or obstructive practices (or any other integrity violations) in any jurisdiction.

Note: *This clause is designed to ensure a Supplier is not subject to Australian targeted financial sanctions and has no history of integrity-related sanctions that could compromise the Customer's probity, security posture or the performance of a Commonwealth contract.*

OFFICIAL

5. Personnel and Subcontractors

Note: *Provisions relating to 'Key Personnel' can be altered to refer to 'Personnel' (and vice versa). Drafters should opt to use the defined term which is most appropriate in the relevant circumstances.*

5.1. [GENERAL RISK] Supplier's Personnel

5.1.1. The Supplier must ensure that the Personnel it uses to perform this Contract:

a) have and apply the skills, qualifications, experience, knowledge and competence necessary to provide the Goods and Services to a standard that complies with this Contract;

b) are of known reliability and integrity;

c) may be reasonably relied upon not to breach the terms and conditions of this Contract, including those relating to:

i. confidentiality;

ii. privacy;

iii. security; and

iv. safety; and

d) do not work for or perform work for other governments or Government Entities (except as advised to the Customer prior to entering into this Contract) without the approval of the Customer.

Note: *This clause provides the Customer with oversight on who will deliver the Goods and Services under a Contract and how that workforce (including subcontractors) will be governed under a Contract.*

Certain Suppliers (for example, those who routinely have Personnel working on contracts for different governments, such as Suppliers who operate in the technology sector) may object to the requirement not to perform work for other governments without the approval of the Customer. It may be necessary to develop a fall-back position, such as requesting a notification (rather than seeking approval) or requesting approval in relation to work undertaken for specified entities (rather than generally). Another option would be to pre-agree which other governments the Supplier is approved to contract to and include this in the contract schedule.

For higher-risk contracts, Customers may wish to specify that Suppliers must ensure that the Personnel they use to perform the Contract meet the Australian Standard for Workforce Screening AS 4811:2022 standard.

5.1.2. The Supplier must:

a) provide any information reasonably requested by the Customer about the Supplier's Personnel;

b) provide suitable replacement Personnel with the skills, qualifications, experience, knowledge and competence needed to perform work under this Contract if any of the Supplier's Personnel:

i. are unavailable;

OFFICIAL

ii. require access to Security Classified Resources but are prevented from having such access under clause 8.6; or

iii. are requested to be removed by the Customer under clause 5.2.1;

c) ensure its Personnel do not do anything which would breach the Supplier's obligations under this Contract; and

d) ensure its Personnel comply with any requirements and directions of the Customer when on or using the Customer's premises or facilities.

5.1.3. This clause does not limit any other obligation on the Supplier.

5.2. [GENERAL RISK] Personnel removal

5.2.1. The Supplier must, at the request of the Customer, promptly remove any of the Supplier's Personnel from work under this Contract at no cost to the Customer. This includes any Key Personnel. The Customer may make such a request at any time, in its sole discretion, and is not required to provide the Supplier with reasons.

5.3. [GENERAL RISK] Subcontractors

5.3.1. The Supplier must not subcontract the provision of any part of the Goods and Services to any Prohibited Entity.

5.3.2. The Customer has approved the subcontracting of the performance of the parts of this Contracts to the Approved Subcontractors stated in the Contract Details. This approval may be subject to conditions notified to the Supplier.

5.3.3. The Supplier must not subcontract any part of the Contract, other than to Approved Subcontractors, unless it has the Customer's prior written approval.

5.3.4. If the Supplier does have approval to subcontract, it must:

a) ensure that all Subcontractors comply with the [[terms of this Contract] or [the following terms of this Contract:

i. agency to insert]];

b) ensure that all Subcontracts contain terms consistent with this Contract, including as required to allow the Supplier to comply fully with the terms of this Contract; and

c) give the Customer details of each subcontract within 5 Business Days of a request by the Customer.

5.3.5. The Supplier acknowledges and must reflect in all Subcontracts that:

a) the Customer may (at any time) revoke approval provided under clause 5.3.2 at any time by notice to the Supplier and is not required to provide reasons;

b) it will make available to the Customer (upon request) details of all Subcontractors engaged in the performance of this Contract; and

c) the Customer may publicly disclose the names of any Subcontractors engaged in the performance of this Contract.

Note: *This clause will only be relevant in circumstances where the Supplier will or may use Subcontractors to perform their obligations under a Contract.*

Customers may wish to require Subcontractors to comply with particular FOCI clauses instead of the whole Contract. In such circumstances, clause a) can be modified to reference particular clauses.

OFFICIAL

5.4. [HIGH RISK] Key Personnel

5.4.1. The Supplier must at all times have in place:

a) contingency plans;

b) succession plans; and

c) other relevant plans, processes and procedures,

to minimise any potential adverse impact for the Customer if any Key Personnel should, for any reason, not be available.

5.4.2. If, despite the best efforts of the Supplier, any Key Personnel becomes (or is anticipated to be) unavailable for any reason, the Supplier must notify the Customer immediately and take all reasonable action to minimise any potential adverse impact for the Customer.

Note: *Customers may wish to use the above clauses to control Supplier Personnel and regulate performance of the Contract. Customers may consider increasing controls for sensitive and/or multi-year services, or decreasing the controls for low-value, short-term procurements that are not sensitive.*

5.4.3. If any Key Personnel:

a) becomes (or is anticipated to be) permanently unavailable or unavailable for a period not acceptable to the Customer;

b) requires access to Security Classified Resources but is prevented from having such access under clause 8.6; or

c) is requested to be removed by the Customer under clause 5.2.1,

the Supplier must:

d) as soon as possible, identify suitably skilled, qualified and experienced potential replacements;

e) provide full written details of the potential replacements to the Customer, including each potential replacement's previous employer;

f) where requested by the Customer, arrange for potential replacements to attend interviews with the Customer and provide requested information about them, to assist the Customer in its consideration of any potential replacement;

g) if the Customer confirms in writing that a potential replacement is acceptable, immediately engage that person and provide them as substituted Key Personnel; and

h) not engage any person as a substituted Key Personnel without the Customer's prior written approval.

5.4.4. The Supplier must use its best efforts to ensure minimal turnover of Key Personnel.

OFFICIAL

6. Digital Systems

6.1. [GENERAL RISK] Remote access to Digital Systems

6.1.1. The Supplier must:

a) ensure that it does not, and does not permit, any unauthorised Supplier Personnel or any Third Party, to access or control any Digital System of the Customer's without the Customer's prior written approval (including by remote access);

b) ensure that no unauthorised attempt is made to access or use, in any way, the Customer's Digital Systems;

c) limit access to the Customer's Digital Systems to Supplier Personnel who:

i. are located within Australia when accessing the Customer's Digital Systems (except with the prior written consent of the Customer);

ii. have been approved by the Customer in writing; and

iii. have a need for such access; and

d) ensure that any access to the Customer's Digital Systems by the Supplier or Supplier Personnel is:

i. limited to the minimum access necessary to enable the Supplier to comply with its obligations under this Contract;

ii. only with the clear identification and recording of the individual gaining access; and

iii. compliant with any other requirements as notified by the Customer.

Note: *This clause seeks to limit remote access to a Customer's Digital Systems to the minimum access necessary to enable a Supplier to comply with its obligations under a Contract with prior Customer approval. Customers may consider increasing controls for high-risk contracts (e.g. by requiring per-session approvals, session recording and/or Australia-based support only).*

Please note that this clause is similar to the DTA Cyber Risk Model Clauses clause on data security and dealing with Buyer data (cl 2.13) – but instead focuses particularly on remote access. Care should be taken to avoid repetition where clauses from multiple model clause banks are being used.

OFFICIAL

7. Compliance with standards

7.1. [GENERAL RISK] Evidence of compliance with standards

7.1.1. The Supplier must ensure that it obtains copies of all relevant certifications and maintains records evidencing its compliance with these standards and promptly provides such copies to the Customer if requested.

Note: *This clause is designed to be added to an existing clause that requires the Supplier to comply with applicable Australian standards, international standards and/or requirements or standards specified in the Statement of Work.*

8. Security

8.1. [GENERAL RISK] General security obligations

8.1.1. The Supplier agrees to provide the Goods and Services in a way that:

a) complies with; and

b) ensures the Customer complies with,

the latest release available prior to the beginning of the Contract, or a subsequent release where agreed to by the Customer, of the:

c) Protective Security Policy Framework;

d) Protective Security Directions; and

e) Information Security Manual.

8.2. [GENERAL RISK] Physical security

8.2.1. The Customer must provide the Supplier access to the Customer's premises and facilities to the extent reasonably necessary (during business hours) to enable the Supplier to perform or provide the Goods and Services.

8.2.2. The Supplier may only use or access the Customer's premises and facilities (including any area licensed to the Customer):

a) if authorised in writing by the Customer; and

b) so long as the Supplier complies with the requirements and procedures of the Customer:

i. as set out in this Contract;

ii. as notified to the Supplier by the Customer from time to time; and

iii. as might reasonably be inferred from the circumstances.

8.2.3. The Customer may deny or suspend the Supplier's access to the Customer's premises and facilities at any time. The Supplier must immediately vacate such premises and cease access if notified to do so by the Customer.

8.2.4. The Customer must, following any denial or suspension of access under clause 8.2.3, allow the Supplier to re-access the Customer's premises and facilities as soon as practicable.

8.2.5. The Supplier is relieved of its obligations under this Contract to the extent that the Supplier is unable to perform its obligations because the Customer denies or suspends the Supplier's

OFFICIAL

access under clause 8.2.3. This clause 8.2.5 does not apply to the extent that the Customer denies or suspends the Supplier's access because of:

a) an act or omission by the Supplier; or

b) any security risk related to the Supplier.

8.2.6. The Supplier must safeguard, and must ensure that its Personnel safeguard:

a) any keys or passes or other relevant access, identification or authentication items or information; and

b) any Material detailing access or security arrangements or that could otherwise compromise security,

that are provided to the Supplier under this Contract.

Note: *This clause governs who, when, how and on what terms Suppliers can access Customer premises and facilities.*

This clause may be suitable where Suppliers are required to access or interface with Customer facilities (including licensed or hosted areas and shared tenancies). Customers may consider increasing protections for sensitive areas (e.g. higher security zones, data rooms or control rooms) by (for example) mandating escorted access and additional security clearances.

Care should be taken to avoid repetition and consistency with existing access and security clauses.

8.3. [GENERAL RISK] External information sharing

8.3.1. The Supplier must not share information about this Contract, the Customer or the Australian Government that is not publicly available with any Third Party without the prior written agreement of the Customer.

Note: *This clause is designed to prevent downstream disclosure of non-public information about Commonwealth contracts, the Customer or the Australian government to any Third Party without the consent of the Customer. This clause is broader than the below clause which relates to Official Information only, and which provides for comprehensive restrictions on the internal treatment of Official Information within Suppliers. This clause (or equivalent confidentiality clauses) should be included as a standard position where FOCI risk is present, unless the Customer and Supplier have separately agreed terms upon which information can be shared with third parties.*

Customers should consider the interaction of these clauses with any existing confidentiality clauses in their Contract.

OFFICIAL

8.4. [GENERAL RISK] Confidentiality of Official Information

8.4.1. Unless otherwise notified by the Customer, the highest level of Security Classified Resources that the Supplier will have access to under this Contract is [agency to insert].

8.4.2. The Supplier must not, without the prior written authorisation of the Customer, disclose any Official Information to any Third Party.

8.4.3. The Supplier does not need the Customer's authorisation to disclose information if the Supplier is required to do so under Australian Law. Where the Supplier is required to disclose Official Information by Australian Law, the Supplier must notify the Customer in writing of the details of the requirement at least five (5) Business Days prior to the required date of the disclosure.

8.4.4. The Supplier must immediately notify the Customer if it considers that it has an obligation to disclose Official Information under a foreign law and provide details of such disclosure requirements. Any disclosure by the Supplier in these circumstances is subject to the reasonable directions of the Customer.

8.5. [GENERAL RISK] Internal sharing of Official Information

8.5.1. The Supplier is authorised to provide access to Official Information to those Personnel and Subcontractors who require access to Official Information for the purposes of properly performing this Contract.

8.5.2. When Personnel and Subcontractors authorised to access Official Information under clause 8.5.1 cease to have require access the Official Information for the purposes of this Contract, the Supplier must ensure that:

a) access to Official Information is removed for such Personnel and Subcontractors; and

b) any Official Information in the possession of such Personnel and Subcontractors is returned to the Supplier and electronic copies are deleted.

8.5.3. The Customer may ask Supplier Personnel or Subcontractors to give a written undertaking not to disclose Official Information. Supplier Personnel and Subcontractors must give the undertaking in a form acceptable to the Customer. The Supplier must arrange for such undertakings to be given when asked.

8.5.4. Any undertaking required should confirm that the requirements relating to the use and non-disclosure of Official Information:

a) continue after the end of the Contract; and

b) survive the expiration of any subcontract or the end of the person's employment with the Supplier.

8.5.5. The Supplier must secure all Official Information that it holds in connection with this Contract against loss and unauthorised access, use, modification or disclosure.

8.5.6. Upon the expiry or earlier termination of this Contract, the Supplier must:

a) return all Official Information in its possession to the Customer and destroy all electronic records of Official Information;

b) ensure that no Personnel or Subcontractors continue to have access to Official Information; and

c) immediately report any non-compliances with this clause 8.5.6 to the Customer.

OFFICIAL

Note: *This clause establishes a regime for Official Information handled under a Contract. The intention of this clause is to prevent Supplier Personnel or Subcontractors from accessing Official Information in the absence of a legitimate need to do so for the purposes of the Contract.*

If undertakings are utilised by the Customer, a register of undertakings will need to be maintained. If this register is not maintained by the Customer, the Customer will require a right to audit the Supplier's register of undertakings.

8.6. [GENERAL RISK] Access to Security Classified Resources

8.6.1. The Supplier must ensure that all Personnel who require access to Security Classified Resources:

a) obtain and hold the appropriate security clearance;

b) comply with Australian Vetting Agency requirements for holders of the relevant security clearance; and

c) comply with reporting requirements applicable to security clearance holders. For example, regarding significant changes to personal circumstances.

8.6.2. The Supplier is responsible for the cost of getting security clearances unless the Customer gives prior written agreement to cover the cost.

8.6.3. The Supplier must:

a) prevent access to Security Classified Resources by Personnel:

i. whose security clearances are revoked or have lapsed; or

ii. who do not have a legitimate and genuine need to access the relevant Security Classified Resources for the purposes of this Contract;

b) make any of its Personnel who require access to Security Classified Resources available to attend any security training provided by the Customer;

c) notify the Customer of any change in the personal circumstances of Personnel referred to in clause 8.6.1;

d) not (either directly or indirectly) perform any part of this Contract outside Australia or permit or facilitate any third party to do so, without the Customer's prior written approval;

Note: *In addition to the following notification requirements, a Customer may require the Supplier provide a Cure Plan if a Security Incident occurs.*

e) notify the Customer immediately if the Supplier:

i. becomes aware that a Security Incident or breach of clauses 8.6.1, 8.6.2, 8.6.4 has occurred; or

ii. reasonably suspects that a Security Incident or such a breach has occurred;

f) implement the Customer's procedures for Security Incident reporting and management as advised by the Customer from time to time; and

g) comply with any additional security requirements notified by the Customer and any variations or additions to those requirements as notified by the Customer from time to time, provided that:

OFFICIAL

i. if the Supplier incurs (or will incur) any material expenses which are directly related to complying with clause g), the parties may negotiate any appropriate variation to this Contract to reflect the Supplier's reasonable and substantiated costs of such compliance. When determining whether an expense is material, the parties will have regard to the total value of this Contract;

ii. unless such variation is agreed between the parties, the Supplier is solely responsible for the costs of complying with clause g); and

iii. the Supplier must not refuse to comply with clause g) or delay such compliance pending the outcome of any negotiations under clause g).i.

8.6.4. The Supplier must implement security procedures to ensure that it meets its obligations under this clause 8.6. The Supplier must provide details of these procedures to the Customer on request.

8.6.5. The Supplier acknowledges that the Customer may treat any failure to fully comply with any of its obligations under this clause 8.6 as a failure that is not capable of remedy.

Note: *Please note that this clause is similar (but not identical) to clause 2.6 of DTA's Cyber Risk Model Clauses. Where those model clauses are also used, care should be taken to avoid repetition and ensure consistency.*

OFFICIAL

9. Termination

9.1. [GENERAL RISK] Termination for fault

9.1.1. The Customer may by notice immediately terminate this Contract or reduce the scope of this Contract (without prejudice to any prior right of action or remedy which the Customer may have):

a) if any information provided by the Supplier during the tender process is found to be incorrect, misleading or incomplete;

b) at the Customer's absolute discretion, following a notification under clauses:

i. 2.2.2

ii. 2.4.2;

iii. 2.4.3; and

iv. 3.2.3;

c) if the Supplier breaches any obligation contained in:

i. clause 2;

ii. clause 3;

iii. clause 5.1;

iv. clause 5.3;

v. clause 6;

vi. clause 7;

vii. clause 8; and

viii. [agency to consider and insert].

Note: *Particular care must be taken to ensure that these clauses do not limit or contradict existing termination provisions. Legal advice should be sought in the event of any uncertainty as to the operation, application or effectiveness of a Contract's termination regime.*

The clauses triggering a right of the Customer to terminate the Contract are suggestions only. Customers should consider which clauses should trigger a termination right in the context of their bespoke procurements.

OFFICIAL

Procurement Contract Model Clause Definitions

Note: *Customers should consider whether each defined term is appropriate when applied to their unique procurement. The suggested definitions below may need to be tweaked or replaced in accordance with each Customer's needs and circumstances, and should be made consistent with the terminology used in the balance of the contract.*

Term	Definition
Approved Subcontractor	means: [agency to insert], or otherwise as approved by the Customer in writing.
Beneficial Owner	means an individual or persons who ultimately own or Control an interest in a legal entity or arrangement, including companies, trusts and foundations. Ownership and control may be direct (such as through shares) or indirect (such as shares held by a Third Party on the individual's behalf).
Change of Control	means when: a) a body corporate, entity or person that Controls (or previously Controlled) the Supplier ceases to Control the Supplier; or b) a body corporate, entity or person that does not Control the Supplier commences Control of the Supplier.
Consolidated List	means the list of individuals and entities listed in the consolidated sanctions list published by the Australian government's Department of Foreign Affairs and Trade.
Contract Details	means the matters described at Schedule [agency to insert].
Contract Period	means the period of this Contract as stated in [agency to insert]. **Note:** *Agencies should consider whether the term 'Contract Period' is appropriate, or whether another term should be used in their Contracts.*
Control	has the meaning given under section 50AA of the *Corporations Act 2001* (Cth).

OFFICIAL

Term	Definition
Digital System	includes any electronic or other system, or any related: a) process; b) equipment; c) tool; d) device; e) infrastructure; f) network; g) data; h) information; i) transmission; j) communication; k) software; or l) facility, whether stand-alone or connected with any other item.
Government Entities	means any: a) department of state; b) parliamentary body; c) organ of the state (including the military and judiciary); d) body corporate that is established and prescribed by Law to be a government entity; or e) body corporate that a government other than Australia Controls.
Information Security Manual	means the Information Security Manual as published by the Australian Signals Directorate, as updated from time to time.
Key Investors and Decision-Makers	means, in relation to the Supplier: a) any person or entity holding, directly or indirectly, more than 20% of the issued share capital or voting rights in the Supplier (including any majority shareholder); b) any shareholder or group of shareholders acting in concert who has the capacity to exercise meaningful control or influence over the management or strategic direction of the Supplier; c) any member of the board of directors (or equivalent governing body) of the Supplier; and d) any Personnel who has, or will have, authority, control or material influence in relation to the decision-making, management and operations of the Supplier.
Key Personnel	means any Personnel approved by the Customer to provide the Goods and Services to the Customer.
Law	means any: a) statute, regulation, rule, by-law, order, ordinance, proclamation, enactment, statutory instrument, binding licence condition or delegated or subordinated legislation that applies or is in operation in the jurisdiction of the Supplier's incorporation; or b) standard, requirement or condition imposed by a Government Entity.
Material	means any thing in relation to which intellectual property rights arise.

OFFICIAL

Term	Definition
Official Information	means any information: a) developed; b) received; or c) collected, by or on behalf of the Customer to which the Supplier gains access under or in connection with this Contract, and includes any Material contained in Goods and Services and the terms of this Contract.
Official Resources	includes: a) Official Information; b) people who work for or with the Customer; and c) assets belonging to (even if in the possession of contracted providers) or in the possession of the Customer.
Personnel or Supplier Personnel	means, in relation to the Supplier, any natural person who is an officer, employee, contracted personnel, labour hire workers, agent or professional adviser of the Supplier or of a Subcontractor, including any Key Personnel.
Prohibited Entity	means any entity that: a) has had a judicial decision against it (not including decisions under appeal) relating to employee entitlements in respect of which it has not paid any judgment amount; or b) is on, or which has any employees that are on, or which is a member of an entity that is on, the Commonwealth's consolidated list of individuals and entities to which terrorist asset freezing applies/
Protective Security Directions	means any directions issued by the Secretary of the Department of Home Affairs under the Protective Security Policy Framework.
Protective Security Policy Framework	means the Protective Security Policy Framework available at www.protectivesecurity.gov.au, as amended or replaced from time to time.
Sanction	means measures imposed on a particular individual, entity, country, group or vessel in response to a situation of international concern. Sanctions take many forms including targeted financial sanctions, travel bans, trade sanctions, and commercial activity sanctions. They may be designed to bring a situation of international concern to an end by influencing those responsible; to limit adverse impacts of a situation; or to penalise those responsible.
Security Classified Resources	means Official Resources that, if compromised, could have adverse consequences for the Customer.
Security Incident	means: a) any actual or suspected breach of security (whether relating to information, personnel, data, logical, physical or system security or otherwise); b) any contact, request or approach from any person seeking unauthorised access to Official Resources; or

OFFICIAL

Term	Definition
	c) any circumstance that highlights any actual or potential security vulnerability or which identifies a potential threat to security.
Subcontractors	means any person engaged by the Seller to provide any part of the Goods and Services under this Contract, and includes Approved Subcontractors.
Third Party	means any entity which is not the Supplier. For the avoidance of doubt, this definition includes entities which are related bodies corporate of (or entities otherwise related to) the Supplier.