Please contact Defence for all Treaty and Australian Community enquiries:

📞 1800 00 57 57
✉️ ustradetreaty@defence.gov.au
## Version control table

<table>
<thead>
<tr>
<th>Date</th>
<th>Change comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 Apr 2013</td>
<td>Initial release</td>
</tr>
<tr>
<td>06 Jun 2013</td>
<td>General &amp; sections 1, 4.2.2, 4.3.1, 7.3, 7.5 and 13.1</td>
</tr>
<tr>
<td>07 Jun 2013</td>
<td>Section 6.1</td>
</tr>
<tr>
<td>01 Jul 2014</td>
<td>General &amp; sections 4.2.1, 4.3.1, 4.3.2,</td>
</tr>
<tr>
<td>24 Oct 2014</td>
<td>General review</td>
</tr>
<tr>
<td>30 Mar 2015</td>
<td>General review</td>
</tr>
<tr>
<td>10 Nov 2016</td>
<td>General review &amp; Sections 4.4</td>
</tr>
</tbody>
</table>
Contents

1. Introduction ............................................................................................................ 5
2. Definitions .............................................................................................................. 6
   3.1. The Approved Community ............................................................................ 7
   3.2. Scope of the Treaty ........................................................................................ 7
   3.3. Governance .................................................................................................... 8
4. Joining the Australian Community ........................................................................ 9
   4.1. Who can join? ................................................................................................ 9
   4.2. Application process........................................................................................ 9
      4.2.1. Application form .................................................................................... 9
      4.2.2. Assessment process .............................................................................. 11
      4.2.3. Foreign ownership, control & influence assessment ........................... 11
   4.3. Handling and storage – Accreditation requirements.................................... 12
      4.3.1. Physical security accreditation ................................................................ 12
      4.3.2. Physical security principles .................................................................. 13
      4.3.3. ICT system accreditation ..................................................................... 15
      4.3.4. ICT system security principles ............................................................. 16
      4.3.5. Security documentation ....................................................................... 17
      4.3.6. Recognition of current security accreditations .................................... 18
      4.3.7. Additional security requirements ......................................................... 19
   4.4. Personnel security requirements .................................................................. 20
      4.4.1. Citizenship requirements ..................................................................... 21
5. Approval or refusal of an application .................................................................. 21
   5.1. Approval conditions..................................................................................... 22
   5.2. Rights of review........................................................................................... 22
6. Operating under the Treaty .................................................................................. 22
   6.1. General ......................................................................................................... 22
   6.2. Transitioning articles into the Treaty........................................................... 24
   6.3. Transitioning articles out of the Treaty........................................................ 24
      6.3.1. Transferring a Treaty Article to a non-Australian Community sub-
            contractor ..................................................................................................... 24
   6.4. Marking........................................................................................................ 25
      6.4.1. How to mark ........................................................................................ 25
      6.4.2. When marking is not practicable ......................................................... 26
   6.5. Record keeping ............................................................................................ 26
7. Compliance and monitoring................................................................................. 27
   7.1. Overview ...................................................................................................... 27
   7.2. Reporting ..................................................................................................... 27
   7.3. Methods for confirming compliance............................................................ 28
   7.4. On-site visit .................................................................................................. 29
      7.4.1. Notice to be provided ........................................................................... 29
      7.4.2. What are Authorised Officers looking for? ........................................... 30
7.4.3. Reasonable assistance ........................................................................... 30
7.4.4. Persons assisting Authorised Officers ................................................. 30
7.5. Requests for information ........................................................................... 30
7.6. Suspension ............................................................................................... 31
7.7. Cancellation ............................................................................................. 31
8. Leaving the Australian Community .............................................................. 32
  8.1. Gaining US authorisations .................................................................... 32
  8.2. Maintaining controls on items ............................................................... 32
  8.3. Retention of Treaty records ................................................................. 32
9. Seizure and condemned articles .................................................................. 33
10. Security awareness and training ................................................................. 33
11. Security incidents and investigations ......................................................... 33
  11.1. Treaty security investigations .............................................................. 34
12. Intermediate Consignees ............................................................................ 34
  12.1. Application process ............................................................................. 35
13. Australian Community member resources ................................................ 36
  13.1. Useful links and resources ................................................................. 36
  13.2. Feedback and comments ................................................................... 36
  13.3. Defence Contacts ............................................................................... 37
1. Introduction

On 5 September 2007 the Australian and the United States (US) Governments signed the Treaty between the Government of Australia and the Government of the United States of America concerning Defense Trade Cooperation (the Treaty). The Treaty is intended to improve the efficiency of eligible two-way transfers between Australia and the US by facilitating the export of controlled goods without the need for an export licence. This was achieved through the creation of an Approved Community in Australia and the US which includes government and private facilities. The Treaty’s Implementing Arrangement (IA) of 14 March 2008, provides the necessary framework for Australia and the US to implement their legal obligations under the Treaty.

The Treaty provides benefits for both Government and defence industry. For Treaty eligible projects, the Treaty:

- reduces delivery time for new defence projects;
- improves sustainment, by permitting transfers within the Approved Community without further Australian or US approvals;
- provides a more efficient way for US companies to share technical data with the Australian Community without licences;
- enables consistent compliance requirements across the Australian Community; and,
- avoids delays sometimes associated with the export licensing process.

Activities within the Treaty’s scope already encompass a substantial part of Australia’s defence trade with the US. The list of Treaty eligible articles and end-uses is expected to expand through use of the Treaty and increased confidence in Treaty processes.

The Treaty is an important addition to Australia’s defence relationship with the US. It provides a mechanism for increased interoperability through more efficient transfers of controlled goods. With over 50 percent of Australian defence imports originating in the US, and extensive existing bilateral cooperation, the Treaty complements pre-existing processes and offers mutual benefit to further strengthen this relationship.

Participation in the Treaty is voluntary, and the Treaty provisions only apply to organisations and individuals who have been approved for membership. Companies experienced in working with the US export controls, particularly the International Traffic in Arms Regulations (ITAR), and classified defence articles (including members of the Defence Industry Security Program (DISP)) should already meet the requirements for membership of the Australian Community (AC).
2. Definitions

Approved Community means the combined Australian Community and US Community. Both communities include respective government agencies and non-government organisations that have been approved as members.

Australian Community (AC) means the Australian government agencies and non-government applicants who have been approved as members of the Australian Community.

Approved Community Identification Number (ACID) means the unique identifier given to each government agency and non-government applicant approved as an AC member. The ACID number must be used as the export permission number for all exports of Treaty Articles from facilities approved for Treaty purposes.

Authorised Executive means a company executive authorised to enter the organisation into contracts or arrangements.

Authorised Officer means a Commonwealth employee who has been appointed under the Act with powers to confirm whether AC members are complying with the conditions of their approval.

Defence Export Control System (DECS) means the Information Technology (IT) system that Defence uses to manage applications and assessments related to Treaty and Defence export licensing arrangements.

Defense Trade Cooperation Munitions List (DTCML) means the list which identifies those defence articles eligible for transitioning into the Treaty.

Exempted Technologies List (ETL) means the list of defence articles that are not eligible for transition to Treaty export or transfer arrangements. Part 2 of the DTCML reflects the content of the ETL.

Intermediate Consignee means any entity or person who has been approved to receive Treaty Articles from an Approved Community member for the sole purpose of transportation and delivery to other Approved Community members, and includes freight forwarders, customs brokers or other commercial transport providers.

Treaty Article means a good, service or technology, controlled for export by the Australian or US Governments, which has been approved or transitioned into the Treaty for transfer to other Approved Community members.

Treaty Trade Officer means an employee of the AC member responsible for contact with Defence and other AC members on Treaty matters.

US Trade Treaty section means the area within Defence responsible for managing the Australian Community.
3. The Australia-US Defence Trade Cooperation Treaty

The domestic legislative authority for the Treaty is provided by the *Defence Trade Controls Act 2012* (the Act) and the accompanying Defence Trade Controls Regulation 2013 (the Regulation).

Together, the Act and Regulation strengthen Australia’s export control laws and provide the legislative framework to implement the Treaty in Australia.

The Act and the Regulation are available on the Defence website.

3.1. The Approved Community

The Treaty creates an Approved Community in Australia and the US to enable members to transfer Treaty Articles without the need for separate export licenses. The Approved Community comprises an Australian Community (AC) and a US Community. The AC is managed by the US Trade Treaty section in the Australian Department of Defence. The US Community is managed by the US Department of State.

For information on membership to the US Community, see the United States Department of State, Directorate of Defense Trade Controls (DDTC) website.

3.2. Scope of the Treaty

The scope of the Treaty is determined by three elements:

1. **Membership** - Any company seeking to transfer articles under the Treaty must be approved as a member of the AC. Treaty Articles can only be transferred between members of the Approved Community unless separate approval under existing export controls is obtained from the relevant Governments.

2. **Eligible articles** - Articles eligible for export or transfer under the Treaty must be listed in Part 1 of the Defense Trade Cooperation Munitions List (DTCML), and not listed in Part 2. Part 2 of the DTCML identifies those articles excluded from transfer under the Treaty and is developed from the Exempted Technologies List (ETL). The ETL is subject to joint determination by both Australia and the United States.

3. **Approved activities** – Four scope lists define the Australian Government and US Government activities under which the transfer of Treaty Articles is permissible. Companies should check whether their current or expected business supports any of the activities covered within the lists:

   - *Combined Operations and Exercises List*: lists eligible military and counter-terrorism operations and exercises that include participation from both Australia and the US.
• **Cooperative Programs List:** lists eligible research, development, production and support programs related to security and defence that involve Australian and US cooperation.

• **Australian Government End-Use List:** lists projects related to security or defence where the Australian Government is the end-user.

• **US Government End-Use List:** lists projects related to security or defence where the US Government is the end-user. Due to the potentially large number of projects a list will not be published. Instead, Treaty eligibility will be identified on the project or tender documentation. Refer to the US Department of State for queries on this list.

The Combined Operations and Exercises List, Cooperative Programs List and the Australian Government End-Use List are available on the Defence website.

### 3.3. Governance

The Treaty will be managed bilaterally through the Australia-US Treaty Management Board comprising representatives from the Australian Department of Defence and the US Departments of State and Defense. The Treaty Management Board provides a forum for discussing the implementation, administration and compliance aspects of the Approved Community as well as the opportunity to share experiences and operational knowledge between the two parties.

The Treaty Management Board’s responsibilities are outlined in the Treaty’s Implementing Arrangement (IA), and include:

- directing activities to effectively implement the Treaty;
- providing clear and relevant guidance on Treaty processes;
- building confidence in the Treaty; and,
- maintaining regular communication between respective governments.

The Management Board will meet annually, or on an as needed basis, and may call upon other government agencies for advice or to take action to implement the Treaty.

In Australia, The US Trade Treaty section in Defence is responsible for managing the AC and day-to-day communications with US counterparts.
4. Joining the Australian Community

4.1. Who can join?

Organisations that currently access, or intend to access, Treaty eligible articles in support of eligible end-uses, may apply for membership to the AC. Organisations that currently access goods or technologies controlled under ITAR may already be involved in eligible business activities. Joining the AC is a voluntary business decision as the potential benefits will apply to some companies more than others.

Entities that choose not to join the Treaty can continue to operate within existing Australian and US defence export controls. Admission does not affect any existing license or business arrangements a company might have.

4.2. Application process

Government agencies

All Commonwealth government agencies, including statutory bodies, can participate in the AC. Commonwealth Government agencies are automatically part of the AC, however they are required to register with Defence so they can be added to the list of AC members.

To register for the AC, government agencies should contact Defence.

Non-government applicants

The application process is a once-off requirement. After approval members can transfer Treaty Articles within the Approved Community without the need to seek further export or retransfer authorisations.

Note: Prior to submitting an application to join the AC, organisations will first have to register as an exporter with Defence and be issued a unique Defence Client Registration Number (DCRN). The registration form is available on the Defence website. The DCRN is only to be used for submitting applications to Defence; and has no relationship whatsoever with an ACID number.

4.2.1. Application form

Non-Government applicants must complete and submit an ‘Application to join Australian Community’ form which is available on the Defence website. The application form requirements include:

- Applicants must attach a signed copy of the Acknowledgment of AC member obligations – see ‘Acknowledgment of Obligations’ below.
- To be eligible for membership to the AC, the applicant will have to meet the requirements described in Section 4.2.2 Assessment process.
- Applicants are required to provide a primary reason for membership on the application form, which may include a description of how their business
activities relate to any of the eligible exercises, programs or projects in the scope lists, or the types of Treaty eligible projects they are seeking to tender or bid for work under.

- Applicants must nominate the facility they will use for the handling, storage or manufacture of Treaty Articles in relation to the membership reason. This facility will be subject to an accreditation process. Accreditation of additional facilities can be requested once membership to the AC has been approved.

In circumstances where a prospective applicant provides services in support of eligible Treaty activities at another company’s or government agency’s facility, they may, with the facility owner’s approval, nominate that facility as their facility for undertaking Treaty activities. For example, if a sub-contractor provides employees to deliver specific services at the contracting company’s premises, and the contracting company’s facility has already been accredited for Treaty activity purposes, then the sub-contractor could nominate the contracting company’s facility as their Treaty facility.

*Note:* This arrangement would only apply if the sub-contractor expects to supply and receive Treaty Articles only at the facility, and separate to the contracting company. The AC member remains responsible for the protection of the Treaty Articles.

**Acknowledgement of Obligations**

Membership of the AC carries legal obligations. This includes standards for reporting and record keeping, and requirements for the marking, handling and storage of Treaty Articles as described in section 4.3 below.

When submitting an application to join the AC, the Authorised Executive is required to sign an acknowledgement of the obligations membership entails. The signed acknowledgement must be attached to the email with their application.

**Authorised Executive and Treaty Trade Officer**

Applicants are required to nominate an Authorised Executive and Treaty Trade Officer from within their organisation. The Authorised Executive must be an individual empowered to enter into legally binding arrangements on behalf of the company. The Treaty Trade Officer is a point of contact for Defence in relation to a company’s activities under the Treaty. Formal notices are addressed to both the Authorised Executive and Treaty Trade Officer.

Email is the preferred method of communication between Defence and AC members.

**Senior Executives**

All persons that hold senior executive positions associated with the applicant (e.g. Board of Directors, or similar governing body, officers, executive personnel, general partners or trustees) must be identified by their full name (given, middle and surname), date of birth, place of birth and citizenship details. These details are required for the Foreign ownership, control & influence (FOCI) assessment (see 4.2.3 Foreign ownership, control & influence assessment).
4.2.2. Assessment process

Non-government applicants
Defence will assess applications to join the AC against the following criteria:

- the organisation’s export compliance history under Australian and US export controls;
- whether the approval of the organisation would prejudice the security, defence or international relations of Australia;
- whether the organisation can demonstrate existing or future involvement in Treaty-eligible activities (against the DTCML and scope lists referenced above);
- the extent of foreign ownership, control or influence over an organisation; and
- whether the organisation has, or has access to, a facility capable of protecting Treaty Articles.

All AC applications will be assessed by the US Trade Treaty section in Defence. If, after assessment, the Australian Government supports the application, applicant details will be provided to the US Government for their agreement.

4.2.3. Foreign ownership, control & influence assessment

All applicants seeking membership to the AC will be assessed against a series of FOCI questions. The applicant’s FOCI assessment must not indicate a possible threat to Australia’s national interest.

The main aim of the FOCI assessment is to minimise the risk of unauthorised access to Treaty Articles by foreign nationals and consists of a two stage process:

1. Identification of foreign nationals who occupy key management positions (this will assist to assess any risk of these personnel accessing Treaty Articles by virtue of their position).
2. Ensuring that measures are in place to reduce the risk of unauthorised access by foreign nationals and/or its consequences.

Stage 2 may involve seeking a signed agreement by the identified foreign national and/or a company representative confirming that access to Treaty Articles will not be sought or provided, and if it does occur, will be reported to Defence.

FOCI responses and facility accreditation requests will be referred internally to the Defence Security and Vetting Service (DSVS) for assessment.
4.3. Handling and storage – Accreditation requirements

Security & protection of Treaty Articles

This manual describes the security standards required for AC members expecting to access controlled unclassified Treaty Articles only.

*Note*: As per existing arrangements, if a company requires access to classified technology they will need to meet the requirements of the Defence Industry Security Program (DISP), administered by the DSVS. Further information on DISP membership is available on the DSVS website. Any Treaty Article classified by the US is automatically accorded an equivalent Australian security classification and therefore subject to the same protection requirements as an Australian classified Treaty Article.

The Treaty and its Implementing Arrangement require that non-government facilities and Information and Communication Technology (ICT) systems used to access or store Treaty Articles are accredited by the Australian Government.

AC members need to ensure that any facilities nominated for the handling, storage and manufacture of Treaty Articles are accredited by Defence. This includes accreditation for both physical security and ICT security.

Government members of the AC are responsible for physical security accreditation of their facilities and ICT systems in accordance with existing Government policy under the Protective Security Policy Framework (PSPF).

4.3.1. Physical security accreditation

The purpose of accrediting applicant facilities is to ensure that appropriate security measures are in place to prevent unauthorised access to controlled unclassified Treaty Articles. Companies that currently access ITAR-controlled technology should already have these measures in place.

Defence, through the DSVS, is responsible for providing physical security accreditation of applicant facilities to meet Treaty requirements for handling controlled unclassified Treaty Articles.

*Note*: For Treaty purposes, a facility may be a floor in a building, a room or an office. Facilities used for the purpose of handling, storage or manufacture of Treaty Articles need to be accredited by the DSVS. Existing Defence facilities are already ‘Approved AC Facilities’ and do not require further physical certification by the DSVS, but applicants must still meet the requirements identified in Principle 3 – Governance and Security Documentation.

Responsibilities for the accreditation process include the following:

- **Applicant:**
  - Certify to Defence that measures are in place to meet the physical security principles outlined in Section 4.3.2 Physical security...
principles through submission of an Unclassified Physical Security Self-Certification form.

- Nominate a point of contact at the facility who has an understanding of the security requirements for the facility.
- Develop or amend security practices and procedures (see 4.3.5 Security documentation) to cover Treaty requirements.
- Maintain security practices and procedures within the facility in accordance with accreditation requirements.

- Defence Security Authority:
  - Assess self-certification documentation completed by applicant.
  - Review applicant’s security governance documentation.
  - Provide an outcome – i.e complete the AC facility accreditation pack or refuse accreditation.

When an applicant seeks membership in the AC only one facility will require assessment for accreditation to conduct Treaty activities. For many applicants this may suffice however, some AC members may request accreditation of additional facilities. An Additional facility accreditation form is available from the US Treaty section.

Reaccreditation of facilities would normally occur either:

- once in a ten year period; or
- on advice received by the member of a major change to ownership or business requirements; or
- in response to security incidents under investigation.

AC members handling and storing classified Treaty Articles will be required to join the Defence Industry Security Program (DISP). Further information on the DISP is available on the DSVS website.

### 4.3.2. Physical security principles

The certification process incorporates risk management principles and physical security measures to achieve the required standard. Applicants are required to self-certify to Defence that they have applied physical security measures, either through technical controls or procedures, to meet the following security principles for the protection of unclassified Treaty Articles.

#### Principle 1. Access Control

Access control systems must be in place to restrict Treaty Article access to only authorised personnel. Controls which support this principle are:

- Procedures and processes to effectively control access to the facility, building or work area to prevent unauthorised access to the treaty articles.
- Commercial mechanical locking devices or electronic access control systems, on site access control, or physical barriers to prevent unauthorised access.
- Visitor Management which includes maintaining a visitor register and escorts.
- After hours access control arrangements.
Where a manufacturing area uses common equipment, this can be temporarily designated by an AC Member as part of their Treaty facility if documented procedures are in place to prevent any unauthorised access while working on Treaty Articles. Once manufacturing is complete, and the Treaty Articles are secured, then the manufacturing area could return to normal use.

**Principle 2. Physical Security**

Provide assurance that the facility or treaty work area meets local government approval standards. Typically, buildings are constructed to the Building Code of Australia and are normally classified as either commercial or domestic. Standard commercial office premises normally provide an increased level of perimeter protection over domestic buildings.

Domestic construction provides little protection from unauthorised access; however, intrusion is generally self evident through forced entry.

In addition to the building code, the facility should be constructed using commercially available locks and keys, or other commercial grade access control mechanisms.

Controls which support this principle are:

- Perimeter walls are constructed of solid material to local government standards.
- Ceilings are of solid construction, or if suspended, have vertical barriers up to the roof to restrict access.
- Any glazing in the facility complies with local government standards.
- All perimeter doors are of sturdy construction and fitted with commercial locking systems.

Whilst not mandatory, physical security may be enhanced with the incorporation of the following product or service types:

- Specialised high-security construction techniques.
- Government tested and endorsed locks or security hardware.
- Security alarm systems.
- Electronic access control systems.
- 24 hour guarding arrangements.

**Principle 3. Governance and Security Documentation (see 4.3.5 Security Documentation).**

Maintain the confidentiality, integrity and availability of controlled information by implementing appropriate measures for the protection of Treaty Articles.

To provide assurance that Treaty Articles are protected, controls which support this principle are:
• Providing clear direction on physical security through the development and implementation of security procedures, orders and plans to address company physical security requirements.
• Prepare a security plan to manage security risks. The security plan must be updated or revised every two years or sooner as changes in risks and the company’s operating environment dictate.
• Develop and implement Security Standing Orders (SSO) or a Technology Security Control Plan (TSCP) which as a minimum contain:
  o Details of any security appointments.
  o Roles and responsibilities of the security appointments.
  o Storage measures for Treaty Articles.
  o Access key management.
  o End of day checks and lockup procedures.
  o Access arrangements, including visitor control.
  o Reporting procedures for security incidents.
  o Reporting procedures for Contact of Security Concern.
  o Local security briefing arrangements for staff.

DSVS can offer advice on how security controls or procedures could be enhanced however, responsibility for applying and maintaining an appropriate level of security to meet the principles remains with the applicant.

The DSVS will validate the Physical Security Self-Certification application and will contact the applicant if further detail or supporting evidence is required to complete accreditation.

Note that failure to provide sufficient detail which demonstrates how each principle is achieved may delay progress of your applicant or require a site visit for confirmation of control measures.

4.3.3. ICT system accreditation

The US Trade Treaty section in Defence is responsible for accreditation of ICT systems at applicant facilities. This is managed through a similar process to the facility accreditation whereby the applicant certifies to Defence that they have measures in place to meet the key ICT system security principles outlined below in Section 4.3.3 ICT system security principles.

The applicant is responsible for determining how each requirement is achieved, either through technical controls or procedures, to ensure that the level of security applied is appropriate to their circumstances.

Note: The Treaty ICT system accreditation described below is only applicable for the access and storage of controlled unclassified Treaty Articles on ICT systems. Applicants with, or requiring, access to official government information or classified Treaty Articles must be approved as a DISP member. To access or store classified Treaty Articles, applicants should contact the DSVS regarding DISP membership and the associated ICT accreditation requirements.
4.3.4. ICT system security principles

Applicants are required to certify to Defence, through the submission of an ICT Self-Certification form, that they have applied appropriate ICT security measures, either through technical controls or procedures, to meet the following security principles for the protection of Treaty Articles.

**Principle 1. Identification and Authentication**

Ensure that access to an ICT system is limited to users and devices that are authorised to access it by using appropriate identification and authentication practices and controls. Controls which support this principle are:

- All terminals with access to Treaty Articles require a password to log-on, or, Treaty Articles are stored separately (isolated on, or external to network) and password protected.
- All terminals auto-lock after 5-10 minutes of inactivity.
- Company has an ICT policy regarding system use and access.

**Principle 2. System Access**

Protect the confidentiality, integrity and availability of information on systems by limiting authorisation to those with appropriate security clearances, briefings and a demonstrated need-to-know. Controls which support this principle are:

- A company ICT administrator controls system access through user authorisation.
- A company ICT administrator ensures that only personnel that have been approved by Defence are permitted to have an account created for access to systems storing Treaty Articles.
  - Ensure the ICT administrator/manager responsible for restricting access to the Treaty Articles.
- Company has an ICT Policy regarding password creation and maintenance.

**Principle 3. Event Logging and Auditing**

Detect and attribute any violations of information security policy by maintaining, auditing and ensuring the availability and integrity of event logs. Controls which support this principle are:

- ICT Operating System (OS) is Windows Vista or later, Linux, Apple or other commercially available OS.
- Security and event logging are enabled.
- Security and event logs are audited on (no longer than) a three monthly basis.

**Principle 4. Software Security**

Maintain the confidentiality, integrity and availability of controlled information and protect against the execution and spread of malware by implementing appropriate software security measures on systems. Controls which support this principle are:

- AVG, Norton, Kapersky, McAfee, AVAST, Trend Micro, Webroot, Panda Security or other approved anti-virus software is installed and enabled.
- Commercially available anti-malware software is installed and enabled
- Automatic updates for anti-virus and anti-malware are enabled.


**Principle 5. Known Software Vulnerabilities**
Maximise software effectiveness and minimise vulnerabilities by implementing and routinely updating preventative measures, such as applying system and software patches, keeping antivirus software up to date and only running supported software. Controls which support this principle are:

- Operating System has automatic updates enabled; or
- Updates are downloaded and installed on a (no longer than) weekly basis.

**Principle 6. Acceptable Use of Mobile Devices**
Prevent mobile devices from becoming a security risk to the system or network they connect to by implementing, and educating personnel on, an effective mobile device usage policy. Controls which support this principle are:

- Company has a policy regarding use of portable devices to reduce security risks.
- Staff using portable devices have read and acknowledged the policy.

ICT accreditation will not specifically require any of the following, although their use would help to increase protection:

- government approved software or hardware devices;
- specialised software of any kind;
- encryption for data storage or transmission; or
- specialised access tokens.

Defence may request to visit an AC member’s facilities to validate a Treaty ICT security self-certification. In such cases, the AC member would be required to demonstrate the features and procedures described in their self-certification.

Defence can offer advice on ways in which security controls or procedures could be enhanced, however responsibility for applying an appropriate level of security to meet the principles will remain with the AC member. In the event that an AC member is unable to demonstrate the measures described in their self-certification, Defence may suspend their AC membership until such measures are in place.

In meeting the security principles, AC members are encouraged to adopt best practice guidance as advised by CERT Australia.

AC members should contact Defence for any queries regarding ICT accreditation requirements.

**4.3.5. Security documentation**

AC members are required to have appropriate documentation outlining the security framework at each of their designated AC facilities. This should include a set of controls, instructions and procedures that detail how a particular security control is implemented in the AC facility.

AC members may have an established document outlining their security controls framework; e.g. *Security Standing Orders* within Defence or a *Technology Security Plan* under the ITAR. AC members may choose to incorporate requirements of the
Treaty into the established document or create an additional annex or appendix as appropriate.

It is recommended that the documentation refer personnel with access to the AC facility to relevant sections of this manual and any applicable security plans to minimise duplication of information.

AC members need to ensure that their security documentation:
- documents their security controls and any approved exceptions;
- accords with applicable security plans;
- is featured as a part of any security awareness activities conducted for their personnel; and
- remains current and readily accessible to relevant staff.

The content of the security documentation will be dependent on each facility’s security environment. The following information may be included:
- details of any security appointments or responsibilities;
- reference to applicable security plans and emergency management plans;
- local security briefing arrangements for staff;
- localised access arrangements, including visitor controls;
- local facility 'close-of-business' checks, lock-up procedures and key management processes;
- internal processes for contact and incident reporting;
- localised storage measures for Treaty Articles;
- local arrangements for the transfer of Treaty Articles; e.g. preferred or contracted Intermediate Consignees;
- any specific requirements for the use of laptops and portable electronic devices;
- listings of prohibited items, if necessary; and
- any localised security awareness regime.

The security documentation should be approved by the AC member’s Authorised Executive.

The AC member is required to ensure that all personnel with access to the AC facility are familiar with the arrangements in the security documentation on commencement of their access, and review them at least annually thereafter or on amendment of the document. These personnel must sign that they understand and agree to the procedures and the AC member must maintain a record of that agreement.

DSVS will provide a template for security documentation to AC applicants and approve the completed documents as part of the physical security accreditation process.

4.3.6. Recognition of current security accreditations

Physical Security

Where an organisation already holds a valid physical security accreditation for a facility under the DISP program, that same facility will meet the physical security
requirements under the Treaty. The proposed Treaty facility will be granted a separate physical security accreditation for Treaty purposes.

**ICT Security**

Where an organisation already holds a valid ICT security accreditation under the DISP program, that same ICT system will meet the ICT security requirements under the Treaty. The AC member would still need to submit their self-certification to Defence and ensure that any Treaty-specific procedures are in place to protect Treaty Articles from unauthorised access.

**Personnel Security**

Australian Government security clearances will be recognised for Treaty purposes, provided that they meet the minimum requirement of BASELINE.

### 4.3.7. Additional security requirements

The security requirements under the Treaty arrangements are the minimum required to ensure the protection of unclassified Treaty Articles. There may be situations where an AC member could be required to implement a higher level of security than required under the Treaty. For example, if handling classified Treaty Articles. Treaty Articles need to be stored in accordance with their classification and while they are not required to be stored separately from other ITAR related goods, the security requirements under the Treaty must be met.

**Unclassified or Classified Official Government Information**

Membership of the AC does not automatically allow AC members to store or handle official government information from either the Australian or United States Governments, regardless of classification.

Similar to non-Treaty activities, if an organisation needs to store or handle official government information in their facilities, specific advice must be obtained from the Defence Security Authority. Membership of the DISP may be required.

**Additional Project-Specific Requirements**

In some cases, a specific Defence project or activity may determine that a higher level of assurance is required. For example, when related operational sensitivities require heightened security protection for the project, or aspects of it.

In these cases, any additional requirements would be placed in contract documentation or other separate agreements, and would be considered separate to AC membership requirements. It would be the responsibility of the contract manager or other person making the agreement to ensure that those additional requirements have been met. Any such additional requirements would not be subject to inspection by Authorised Officers checking compliance with Treaty requirements.

**Other requirements**

Further conditions may be imposed on AC members based on DSVS assessments. Applicants will be advised if any changes are required to facilitate approval.
4.4. Personnel security requirements

All AC member personnel requiring access to Treaty Articles must hold a minimum Australian Government BASELINE security clearance. Where Treaty Articles are classified above RESTRICTED all personnel requiring access to those articles must hold a commensurate security clearance.

AC members querying existing clearances or requiring new or upgraded clearances for their personnel for the purpose of the Treaty should contact Defence Export Controls Branch (Tel: 1800 661 066) in the first instance. All clearance applications require a Defence sponsoring authority. Baseline clearances will likely be sponsored by Defence Export Controls Branch. Clearances above Baseline will likely be sponsored by the specific Defence project area requiring the classified articles. In determining whether to sponsor a security clearance, Defence will consider the position of the nominated applicant and their requirement to access Treaty Articles. It is government policy that the number of people requiring security clearances to perform their duties is kept to a minimum.

Security clearance services for the Australian Government are provided through the Australian Government Security Vetting Agency (AGSVA). Details on the application process can be found at the AGSVA website (www.defence.gov.au/AGSVA/Default.asp). Once a determination has been made by Defence to sponsor an applicant, Defence will advise AGSVA to provide a clearance application pack (e-pack) to that individual. It is the individual’s responsibly to complete the e-pack in the required timeframe and source the required documentation.

All costs payable to AGSVA for the purpose of obtaining a security clearance will be borne by the AC member. Defence does not fund AC member personnel to obtain required clearances. Details and possible exceptions regarding AGSVA charges for Defence Industry vetting services can be found at the following website www.defence.gov.au/AGSVA/industry-qa.asp

Managing security clearances

An AGSVA security clearance requires continued safeguarding by both the individual and AC member post issue. These responsibilities will be communicated upon issue and further detail can be found at www.defence.gov.au/AGSVA/maintaining-your-clearance.asp

The AC member’s security point of contact must maintain a record of security clearances held by all personnel within their area of responsibility. Any security concerns, including attempts by external parties to cultivate AC member’s personnel or acquire Treaty Articles and associated information without authorisation are to be reported to the Defence Security and Vetting Service (DSVS) (www.defence.gov.au/DSVS).
Contact reporting
AC personnel are asked to report contacts of security concern to assist in the identification of any attempts by external parties to cultivate AC member personnel or to acquire Treaty Articles and associated information without authorisation. Contact reports are to be made to the DSVS at security.incidentcentre@defence.gov.au

Security training and incident reporting
AC members are to ensure that their employees maintain security training and awareness requirements, including an understanding of incident reporting processes.

4.4.1. Citizenship requirements
AC member personnel who require access to Treaty Articles must be Australian citizens. This requirement may be waived with the agreement of both the Australian and US Governments.

A waiver would only be granted in exceptional circumstances. For example, a waiver may be granted when an activity requires specialised skills or expertise which the subject possesses and no, or limited, Australian Citizens possess similar capability.

A request for a citizenship waiver should be submitted to Defence prior to seeking a personnel security clearance. Defence will review the request and coordinate with AGSVA for a citizenship waiver to seek an Australian Government personnel security clearance and then liaise with the US to seek approval. Applicants who wish to seek a citizenship waiver should contact Defence for details.

Foreign Government security clearance recognition
Personnel who are citizens of the United States, United Kingdom, Canada, or New Zealand, and who hold a current and valid personnel security clearance issued by the Governments of these countries, can apply to Defence to have recognition of their clearance accepted. In these cases, a citizenship waiver would still be required.

Applicants seeking to have Foreign Government security clearances recognised should contact Defence for guidance.

5. Approval or refusal of an application
If an application is approved, the applicant will receive a notice advising of their approval as a member of the AC along with details of their ACID number. The ACID number and organisation details will be held in a database of Approved Community members. A list of AC members is published on the Defence website. An AC member can elect to not be included on the list.

If an AC application is refused, the applicant will receive a notice which includes the reason/s for refusal. Any applicant who is refused AC membership may seek to have the decision reviewed. See Section 5.2 Rights of Review.
5.1. Approval conditions

The standard conditions of membership will be listed on the notice of approval. An AC member must continue to comply with all conditions throughout their membership. In rare circumstances Defence may include additional conditions on AC members.

5.2. Rights of review

An applicant who has had their application to join the AC refused, and is dissatisfied with that decision, may request to have the decision reviewed by the Minister for Defence. A request for review of a decision must be made in writing and provided to the Minister within 30 days after the applicant was advised of the decision. The request for review must set out the reasons why the applicant is dissatisfied with the decision.

If an applicant is still dissatisfied with a decision after it has been reviewed by the Minister they may apply to have the decision reviewed by the Administrative Appeals Tribunal.

6. Operating under the Treaty

6.1. General

AC members must ensure that all facilities and ICT systems intended for the storage, handling and manufacturing of Treaty Articles have been accredited by Defence in accordance with Section 4.3 Handling and storage – Accreditation requirements, and that all personnel who require access to Treaty Articles meet the requirements of Section 4.4 Personnel security requirements.

Transferring Treaty Articles

Before transferring any Treaty Article using Treaty arrangements an AC member must ensure that:

- the Treaty Articles intended for transfer are eligible under the DTCML;
- the transfer is in support of an eligible project, program, exercise or operation;
- the Treaty Articles are being supplied from and/or transferred to members of the Australian or United States Community only;
- all employees who will gain access to Treaty Articles are Australian citizens, or have been granted an Australian citizenship waiver;
- all employees who will access Treaty Articles hold a current BASELINE or higher personnel security clearance issued by the Australian Government;
- a process is in place to make a record of the transfer that meets the requirements of the Defence Trade Controls Regulation;
- only approved Intermediate Consignees or other Approved Community members are used to transport Treaty Articles;
- Treaty Articles are properly marked (see Section 6.4 Marking);
- ICT systems used for the storage or accessing of Treaty Articles are accredited by Defence;
• the facility used for the storage, handling or maintenance of Treaty Articles is accredited by Defence;
• any changes to Foreign Ownership Control or Influence, company structure or senior executives have been reported to Defence; Treaty Articles are packaged to ensure markings are not visible to unauthorised persons; and,
• any other regulatory requirements prescribed by the Australian Customs and Border Protection Service (ACBPS) have been considered by the AC member.

Confirming Approved Community membership status
Prior to supply, AC members need to confirm if the entity receiving the Treaty Article is a member of the Approved Community.

• To confirm AC membership - The AC member should request the recipient’s ACID number and if required, may seek validation from Defence by emailing ustradetreaty@defence.gov.au.
• To confirm US Community membership - The AC member should request written confirmation of their registration with DDTC.

A record of the confirmation should be retained by the AC member.

Export, import and domestic transfers
The AC member should follow all general regulatory requirements prescribed by the Australian Customs and Border Protection Service (ACBPS) for the export or import of controlled goods.

Export permission (from the Defence Export Control Office) is not required for the export of Treaty Articles to US Community members or deployed Australian Community members such as Defence. However, the supplying AC member must quote their ACID number as the export permission number for all exports conducted under the Treaty.

An AC member can only provide a Treaty Article to an approved Intermediate Consignee or another Approved Community member for the movement or export of the article.

Disposal / Destruction
The disposal or destruction of any Treaty Article will require a record of the activity to be made for audit purposes. Where the Treaty Article is identified as Significant Military Equipment, Defence must be advised of the destruction.

If an AC member uses an external service provider for the disposal or destruction of Treaty Articles, that service provider must be a member of the Approved Community.

Changing the end-use of a Treaty Article
If an AC member wishes to transfer a Treaty Article in support of a different Treaty eligible end-use than that for which the article was originally transitioned, this must be recorded in sufficient detail to allow Defence to track the article’s movement as required to ensure compliance. This may occur in a range of circumstances, for example, when a Treaty eligible project has concluded but the Treaty Articles can be used in support of a different Treaty eligible project.
6.2. Transitioning articles into the Treaty

Only defence articles that have been supplied under a licence arrangement will need to be transitioned into the Treaty and approved as eligible for transfer under the Treaty arrangements. Normally, Treaty articles will be transitioned into the Treaty by the Original Equipment Manufacturer, generally a US Community member. An AC member should only need to request transition of an article into the Treaty if the article in question has been exported from the US under an ITAR licence and is currently located in Australia.

In the first instance, AC members should request the US Community member who originally supplied the article to transition it to Treaty arrangements. If required, Defence will coordinate with the US Government to confirm the eligibility of the article for transition.

AC members wishing to transition Australian Government end-use articles into the Treaty can apply to Defence. Treaty Articles only need to be transitioned into the Treaty once. Application forms are available on the Defence website.

6.3. Transitioning articles out of the Treaty

AC members may decide to have Treaty Articles in their possession transitioned out of the Treaty.

To transition an article from the Treaty, the AC member should apply to the US DDTC for any specific authorisations required to transfer the articles to recipients outside the Approved Community.

Export authorisation would also be required from the Defence Export Control Office prior to the export of the articles from Australia.

The transition of the article from the Treaty to another export authorisation should be recorded by the AC member.

6.3.1. Transferring a Treaty Article to a non-Australian Community sub-contractor

AC members may have reason to temporarily transfer Treaty Articles to an entity that is not a member of the Approved Community for maintenance or other services. There are several options available to do this without having to transition the Treaty Article out of the Treaty.

Firstly, an AC member may seek authorisation from the US Government to transfer the articles through an ITAR 123.9 retransfer General Correspondence Letter. After US approval, and whilst in the other entity’s possession, the Treaty Article will be subject to normal ITAR access requirements and will only become Treaty controlled again after it is returned to the AC member. This allows AC members to retain business with companies that are not members of the AC without requiring separate authorisations, such as a Manufacturing License Agreement or Technical Assistance Agreement.
AC members can apply directly to the DDTC for approval of the General Correspondence Letter, rather than through the original exporter. However, AC members considering a General Correspondence Letter should first contact Defence for guidance.

Another option would be to seek authorisation under existing access arrangements, such as Manufacturing License Agreement or Technical Assistance Agreement, and transfer the articles under their authority.

### 6.4. Marking

All Treaty Articles must be marked in the manner described below to clearly identify them as Treaty Articles. This includes documents and emails that contain controlled information.

<table>
<thead>
<tr>
<th>For US Origin Treaty Article</th>
<th>For Australian Origin Treaty Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted USML//REL AUS and USA Treaty Community</td>
<td>Australian unclassified USML//REL AUS and USA Treaty Community</td>
</tr>
</tbody>
</table>

The term 'Restricted' in the marking of an unclassified controlled US origin Treaty Article is intended as a marker indicating that access is restricted to members of the Approved Community. It is not a security classification.

Where the Treaty Articles are classified, AC members must also be members of the Defence Industry Security Program (DISP) and meet the protective security handling requirements of the classification. The marking requirements for classified Treaty Articles differ from the above. AC members accessing or transferring classified Treaty Articles should contact DSVS for marking requirements.

**When to apply, when to remove**

A Treaty Article should already be marked if it is received as a Treaty Article.

An AC member should mark a Treaty Article if they have received approval to transition it into the Treaty.

If an AC member receives a Treaty Article that is not marked correctly, or not marked at all, they are required to correct the marking and report this to Defence as soon as reasonably possible.

### 6.4.1. How to mark

AC members can use whatever method they prefer to best apply the marking to Treaty Articles. There is no standard that must be adhered to.
6.4.2. When marking is not practicable

If it is not practicable to mark a Treaty Article, perhaps because of its fragility, precision, functionality or composition, or if the Treaty Article is intangible, it must be accompanied by documentation that is marked in the manner explained above. Documentation which may be marked to identify the article as a Treaty Article includes, but is not limited to, bills of lading, invoices and shipping bills.

Electronic transfers of Treaty Articles must carry the required marking within the electronic format, for example, in the subject line of an email or in the file name.

These marked documents, or copies, must be kept in accordance with the AC member’s record keeping requirements.

Intangible transfers of Treaty Articles that are verbal in nature, such as training courses or presentations, should be preceded by a verbal identification of the marking, which serves the same purpose as marking.

6.5. Record keeping

AC members are required to keep records of all activities conducted under the Treaty and keep those records for a minimum of five years. These records may be subject to compliance monitoring verifications as referred to in Section 7 Compliance & monitoring.

Provided that the necessary information is recorded, there is no specific record keeping system or type of record that is required. For example, email correspondence that identifies the information below may be used as a record for the purposes of a Treaty transfer.

The types of activities to be recorded include all instances where Treaty Articles are supplied to Approved Community members or other recipients, or where an AC member conducts an activity related to Treaty Articles as a result of a direction issued by Defence. The types of information that need to be recorded are:

- a description of the Treaty Article(s);
- the ACID number of the AC member;
- the date, time and place from which the Treaty Articles were supplied;
- the name of the approved Intermediate Consignee or Approved Community member used to transport the Treaty Articles and the date the Treaty Articles were supplied to them;
- the name of the Approved Community member to whom the Treaty Articles were supplied (the receiver) and the date, time and place that the Treaty Articles were received;
- for electronic transfer of Treaty Articles, sufficient details to identify the transfer are required, such as a copy of the email which supplied Treaty Articles; and
- the marking applied to the Treaty Articles or accompanying documentation.
7. Compliance and monitoring

Defence will conduct compliance monitoring in consultation with AC members to confirm that AC members are meeting the conditions of their membership.

7.1. Overview

Australian Community members are required to meet certain record-keeping, reporting, access restriction and other membership conditions as part of their requirements for continued membership of the Australian Community. These conditions ensure the protection of Treaty Articles and support the Government’s export controls on defence technology.

7.2. Reporting

Annual compliance report

All Australian Community members are required to submit to Defence an annual compliance report within 30 days of the end of the Australian financial year (30 June) regardless of the number of Treaty transfers that have occurred.

The report should be endorsed by the Treaty Trade Officer or Authorised Executive and should include a statement to confirm the AC member’s compliance with the Act, Regulation and membership conditions. Known or suspected security incidents are to be included in the AC member’s annual compliance report.

Note: A template for the annual compliance report will be emailed to all AC members before the end of the Australian financial year.

A report to DSVS in relation to security assurance and security performance monitoring will also be required as part of the annual compliance reporting process.

Reporting material changes

Where possible, AC members should report immediately to Defence any material change to the information originally supplied in their application to join the AC. A material change may include: a change in the senior executives or the registered address of the company; acquisition or divestment of a subsidiary or foreign affiliate; a merger; or a take-over. If any of the information supplied to Defence in the ‘Application to join the Australian Community’, or any other information on which the AC membership approval is made, changes, then Defence must be notified of the change.

Changes to FOCI or security status are also examples of material change.

FOCI changes

AC members are required to report any changes that may affect their FOCI assessment at least 60 calendar days in advance of the change. Examples of changes to FOCI include a change of ownership or a change to senior executive personnel. Once the change has occurred, AC members are required to report the details of the change to Defence, within five days of the change.
Security changes
AC members are required to report immediately to Defence any changes to their personnel, facilities or ICT systems that may affect their ability to maintain accreditation for the purposes of the Treaty.

7.3. Methods for confirming compliance

Defence will use a variety of monitoring activities to confirm that members of the AC are adhering to their Treaty obligations. For example, in addition to reviewing annual reports Defence may, as necessary, choose to conduct an on-site monitoring activity or request reports or information on the operation of Treaty activities and relevant business or personnel changes.

In the event of actual or suspected non-compliance being identified, the first priority for Defence is to ascertain how the incident occurred, the potential risks posed by the incident, and what, if any, measures have been taken to ensure a similar incident does not recur.

For minor violations, Defence will provide guidance to the AC member on how to prevent recurrence. Defence may also undertake further measures to ensure the AC member is meeting the conditions of their membership approval. For example, reporting requirements may be increased to maintain visibility over a continuing issue of concern, or internal procedures may require modification or improvement to retain membership.

For violations of a more serious nature, repeated minor violations, or where it is obvious that the intent of the AC member was to not comply with membership requirements, Defence may choose to take more direct action. In that regard, the Act provides Defence with the power to suspend or cancel an AC membership in certain circumstances.

While these powers will not be used lightly, membership of the AC is conditional on continued compliance with membership obligations, and if these are not met then membership may be revoked, either temporarily or permanently.

The Treaty requires Defence to report repeated or serious violations to the US Government.

In the most serious cases, Defence may refer the matter to the Australian Federal Police or the Australian Customs and Border Protection Service for further investigation.

Further information on Defence’s approach to managing compliance is provided in the Treaty Compliance Policy available on the Defence website.
7.4. **On-site visit**

An Authorised Officer may conduct on-site monitoring at any reasonable time of day to confirm that AC membership obligations have been met in accordance with the Act and its Regulation. Except in certain circumstances requiring prompt action, Defence will ensure that on-site visits are scheduled within standard business hours and at a reasonable time.

Where an on-site monitoring activity is to be conducted, a minimum of 24 hours notice will be provided to the AC member prior to the visit. The notification will also include sufficient detail to allow the AC member to identify the Authorised Officer who will conduct the on-site monitoring activity.

**Authorised Officers**

Authorised Officers are Defence officials from the US Trade Treaty section that have been provided inspection powers under the Act. These powers may only be used in relation to confirming compliance with Treaty requirements.

The primary role of the Authorised Officer is to provide advice and assistance to the AC member to support their compliance.

An Authorised Officer will carry an identification card that identifies them as an Authorised Officer for the purposes of the Act. An AC member is entitled to request the Authorised Officer to show their identification card before they allow the Authorised Officer access to their facility.

To identify if an AC member has complied with their membership, record keeping or other approval conditions an Authorised Officer may:

- search, inspect, examine, or conduct tests of anything on site (including electronic equipment);
- make recordings of any thing on the premises;
- inspect and make copies of any documents, including electronic records, or operate electronic equipment;
- take any equipment and materials required to exercise monitoring powers onto the premises; and
- in certain circumstances, secure anything for up to 24 hours.

**7.4.1. Notice to be provided**

Defence will attempt to provide the AC member’s Authorised Executive with as much notice as possible, but at least 24 hours prior, to the commencement of any on-site visit.

The regularity of monitoring activities may vary according to, for example, the volume of transfers under the Treaty or the compliance history of the AC member.
7.4.2. What are Authorised Officers looking for?

Where necessary, Authorised Officers will undertake inspections of records and premises to assess the AC member’s compliance with the conditions of their AC membership approval. Specifically, Authorised Officers will, for example, ensure that: records have been kept accurately; Treaty Articles are appropriately marked, handled and stored; and, access to Treaty Articles is restricted in accordance with the Act and its Regulation.

7.4.3. Reasonable assistance

The Treaty Trade Officer (or in their absence, a suitable substitute) should facilitate the visit and provide reasonable assistance to the Authorised Officer. An AC member is obliged to provide access to facilities and will be required to answer questions or provide documents relating to the purpose of the visit. Authorised Officers will advise AC members of any specific requirements prior to commencing a monitoring activity. A representative of the AC member is entitled to observe the inspection but can not impede the Authorised Officer in their duties.

7.4.4. Persons assisting Authorised Officers

In certain circumstances an Authorised Officer may require the assistance of another person to undertake their duties. A person assisting the Authorised Officer may enter the premises and exercise monitoring powers in relation to the premises under the direction of the Authorised Officer. Any power exercised by a person acting under the direction of an Authorised Officer is taken to have been exercised by the Authorised Officer.

Persons assisting an Authorised Officer may include other Defence employees, Customs officers, other Government officials or US Government officials.

7.5. Requests for information

What may be sought?

Under the Act, Defence has been granted the power to request information from AC members in relation to their activities under the Treaty. Defence may use this power to confirm data accuracy within reporting material provided to Defence or to obtain information regarding suspected non-compliance.

Examples of the information or records an AC member may be requested to provide are:

- information regarding companies with whom the AC member does business;
- an inventory of Treaty Articles in the AC member’s possession;
- Treaty Article import and export history;
- evidence of access controls; or
- any other information relevant to the AC member’s compliance with their conditions of membership approval.
7.6. Suspension

Provisions within the Act provide Defence the power to suspend an Australian Community member for a specified time if the AC member:

- has contravened a provision of the Act;
- has breached a condition of the approval;
- holding the approval prejudices the security, defence or international relations of Australia;
- provided information in their application for membership to the AC that was false or misleading; or
- circumstances change from those which existed at the time of approval.

What to do if suspended?

Suspension provides the Australian Community member with an opportunity to implement processes and policies, or amend an existing practice deficiency in order to have the suspension lifted. In accordance with the Act, Defence will provide an AC member with a notice of suspension. The notice will come into force at the time the AC member receives the notice and will request the recipient to take a specified action, or not to take a specified action, in relation to the Treaty Articles in their possession at the time of suspension.

Can Treaty activities continue if suspended?

While an AC member is under suspension, they are not permitted to undertake any activities under the Treaty. The suspension notice will identify a suspension timeframe of 60 calendar days and any conditions required to be met before the AC member can seek to have the suspension lifted. The suspension can only be lifted when all conditions of the suspension have been met. Defence can renew the suspension if conditions are not suitably improved within the initial timeframe and another suspension period of 60 calendar days may commence. If an AC member does not make efforts to meet the conditions for the lifting of a suspension, Defence may seek to cancel their AC membership.

AC members will be required to comply with Treaty Article access control requirements for the duration of any suspension.

7.7. Cancellation

In circumstances of serious or repeated non-compliance, the Minister for Defence may decide to cancel an AC member’s membership. For a cancellation to take effect, Defence will issue the AC member a notice of cancellation. The notice comes into force at the time the organisation receives the notice and will request the company to take a specified action, or not to take a specified action, relating to the Treaty Articles in their possession at the time of cancellation.

What to do if cancelled?

Cancellation of AC membership will remove permission to undertake any activity under the Treaty, including the handling, storage, manufacture or supply of Treaty Articles. Former AC members need to ensure that they continue to meet handling and
storage requirements for Treaty Articles until other authorisations for the possession
and/or supply of the articles are in place.

**Getting authorisations in place**

Organisations that have had AC membership cancelled should apply for other relevant
authorisations from DDTC, and the Defence Export Control Office prior to export.

**8. Leaving the Australian Community**

Organisations wishing to withdraw their AC membership should notify Defence of
their intention. An application to cancel AC membership will then be provided which
the organisation will need to complete and return to Defence. Members will need to
obtain licences or other authorisations for all Treaty Articles in their possession before
their removal from the AC can be finalised.

AC members who no longer require access to Treaty Articles in their possession may
seek to return the articles to the supplying Approved Community member or transfer
them to another Approved Community member before they leave the AC.

Once removal from the AC has been processed, the organisation will no longer be an
AC member, and will not be able to conduct activities under the terms of the Treaty.
Any ACID numbers registered to that organisation will be invalidated.

**8.1. Gaining US authorisations**

Organisations that have left the AC, or had their membership cancelled, will need to
apply to the DDTC through their US supplier for the relevant US export or retransfer
authorisations if they require continued access to US defence articles.

Please contact Defence for further advice and assistance if required.

**8.2. Maintaining controls on items**

Until other valid licences or authorisations are obtained to replace AC membership
obligations, organisations formerly registered under the AC are required to maintain
Treaty-equivalent access control on all Treaty Articles.

**8.3. Retention of Treaty records**

Any organisation that was formerly registered as an AC member is required to retain
records of all Treaty activities for a minimum of five years after the date of the Treaty
activity.
9. Seizure and condemned articles

If an AC member supplies, or attempts to supply, any Treaty Article in contravention of the Act, the article and anything in which it is contained, is forfeited to the Commonwealth and the matter may be taken to Court for resolution.

Where a Treaty Article is forfeited to the Commonwealth, Defence may refer the matter to the Australian Federal Police, a member of a State or Territory police force or a Customs officer to seize the article.

Treaty Articles involved in a contravention of the Act may be condemned and subsequently, could be destroyed in accordance with Defence directions.

10. Security awareness and training

Security awareness and training programs promote and support effective protective security, and participation results in strengthening the security culture of members of the AC.

Government members are responsible for providing security awareness and training to their AC personnel.

AC members are encouraged to develop and implement a security awareness program. DSVS can provide a core element of this program that members could supplement with awareness of local security instructions and procedures.

AC members are encouraged to maintain a record of all AC personnel participating in security awareness and training programs.

11. Security incidents and investigations

Security Incident Reporting

AC member personnel should immediately report all actual or attempted thefts involving Treaty Articles to their State or Territory police and DSVS, and advise their security point of contact.

Non-government members of the AC are to report all known or suspected security incidents that may affect their physical security accreditation to the Security Incidents Centre (SIC) (see Section 13.3 Defence Contacts). The SIC will assess all security incident reports and determine if an investigation is required.

Procedures for the reporting of security incidents should be contained in the facility’s security documentation.
11.1. Treaty security investigations

Non-government AC members:
In the event of a known or suspected security-related incident involving a non-government AC member, DSVS may conduct a security investigation.

The AC member and personnel are required to cooperate with authorities in the course of an investigation into any known or suspected security incidents. Recommendations will generally be made as an outcome of investigations to minimise the chance that the incident reoccurs. The AC member should implement any recommendations within three months and advise DSVS accordingly.

If recommendations cannot be implemented within three months, the AC member’s Authorised Executive is required to:
- notify DSVS in writing;
- negotiate an alternate timeframe with DSVS; and
- implement all recommendations within the agreed alternate timeframe.

DSVS will conduct reviews as necessary of security incident reports involving Treaty Articles and report these findings to the US Trade Treaty section in Defence.

Government Agencies:
Government members of the AC are responsible for conducting agency security investigations and reporting the outcomes to Defence.

12. Intermediate Consignees

Eligibility
An Intermediate Consignee is any entity or person who receives Treaty Articles from an AC member for the sole purpose of transportation and delivery to other Approved Community members. Freight forwarders, customs brokers or other commercial transport providers seeking to transport Treaty Articles can apply to become an Intermediate Consignee. To be eligible, the primary business of the applicant must be as an intermediate consignee, and they must have a tracking system able to identify the location of a Treaty Article in their possession and to record delivery details.

An Intermediate Consignee’s only activity involving Treaty Articles is the facilitation of movement between Approved Community members. An approved Intermediate Consignee is not required to join the AC.

All Intermediate Consignees will be identified on the Approved Intermediate Consignee List on the Defence website. AC members are only permitted to supply Treaty Articles to Intermediate Consignees for the purpose of transportation and delivery to other Approved Community members.
12.1. Application process

Entities or persons seeking to become approved Intermediate Consignees should submit an ‘Application to become an Approved Intermediate Consignee’ form available on the Defence website.

Business Requirements

The primary business of an Intermediate Consignee applicant must be as a freight forwarder, customs broker or other commercial transport service provider. Defence will assess an applicant’s suitability based on information provided in the application.

Tracking System

An Intermediate Consignee must be capable of tracking the movement of Treaty Articles in their possession, including the ability to:

- identify the location of an article in their possession;
- record the date and the time the article is received;
- record the date and the time the person delivers the article;
- identify the person to whom the article is delivered; and
- record the place at which the article is delivered.

The specific requirements are detailed in Section 20 of the Regulation.

Approval Conditions

Approval as an Intermediate Consignee is subject to the applicant continuing to meet the approval conditions. The company name and business contact phone number will be included on the Approved Intermediate Consignee list, which will be available on the Defence website.

All conditions of approval will be included on the Notice of Approval which will be supplied to the Intermediate Consignee if their application is approved.
13. **Australian Community member resources**

Defence has established several support systems for Australian Community members and interested persons. A US Trade Treaty website has been published and is regularly updated to ensure the information remains relevant and current.

Members of the US Trade Treaty section are available during business hours for enquiries via email or telephone (see 13.3 Defence Contacts).

Outreach activities are generally published on the US Trade Treaty website and training programs may be considered upon request by members of the AC.

### 13.1. Useful links and resources

The Defence US Trade Treaty website hosts general Treaty information for AC members, Intermediate Consignees and potential applicants, including:

- Treaty Implementing Arrangement.
- Frequently Asked Questions.
- Resources and Guidance for Australian industry and Government.
  - Treaty application forms
  - Treaty end-use (scope) lists
  - Australian Community member list
  - Approved Intermediate Consignee list
  - Compliance Policy
  - Australian Legislation
    - Defence Trade Controls Act 2012
    - Defence Trade Controls Regulation 2013
    - Defense Trade Cooperation Munitions List
  - US Legislation
  - General Treaty information

The most recent version of all resources will be available on the US Trade Treaty website.

### 13.2. Feedback and comments

Defence is committed to providing the best possible support for the Australian Community and strongly encourages your feedback to ensure the Treaty’s collaborative success. If you have any comments on this manual, the website, telephone or email support services, or if you have any comments or queries on any aspect of the Treaty or Australian Community, please contact the US Trade Treaty section using the contact details in Section 13.3 Defence Contacts.
### 13.3. Defence Contacts

<table>
<thead>
<tr>
<th>Contact Area</th>
<th>Contact for issues relating to:</th>
</tr>
</thead>
</table>
| US Trade Treaty section | ● Australian Community membership  
● All Compliance matters  
● Authorised Officer powers  
● Sponsorship of personnel security clearances  
● Sponsorship of additional facility security accreditations  
● AC membership confirmation  
● ICT self-certification  
● Physical Security self-certification  
● Transition article to Treaty  
● Marking for Treaty Articles  
● Recordkeeping  
● Reporting  
● Support resources & feedback  
● Destruction of Treaty Articles |
| Email: ustradetreaty@defence.gov.au  
Ph: 1800 66 1066; +61 26266 7222 (when outside Australia)  
| Defence Security And Vetting Service  
● FOCI issues  
● Enquiries relating to ‘Classified’ Treaty Articles  
● DISP membership |
| Protective Security Advice Desk:  
Ph: 1300 127 722 | ● Incidents concerning security breaches, losses, or theft  
● Contact reporting |
| Security Incident Centre  
Ph: 02 6266 3331 | ● Personnel security clearance (for existing clearances or clearances in progress) |
| Australian Government Security Vetting Agency  
Email: securityclearances@defence.gov.au  
Ph: 1800 640 450 | ● Export licence applications for DSGL controlled goods and technology |
| Defence Export Controls Branch  
Email: ExportControls@defence.gov.au  
Ph: 1800 66 10 66 ; +61 26266 7222 (when outside Australia)  