The Australian Industry Group

Australian Guide to Export Controls and Best Practices

December 2016

AiGROUP

The Australian Industry Group

Australian Guide to Export Controls and Best Practices

A guide for Australian companies, researchers and academic institutions handling defence and dual-use controlled goods and technology subject to Australian and U.S. export controls.

Last updated: 19 December 2016

Acknowledgements:

The Guide has been completely revised by the Best Practices Working Group of the Australian Export Control Forum. Working Group participants are experienced practitioners in the export/import control arena and have provided their time and input to complete the guide. Current participants included;

Jurgen Zacny – Thales Australia (Editor and Chair)

Eva Galfi – International Trade Advisors (Editor and Contributor)

Zoran Franicevich - Thales Australia

Julia Reed – Northrop Grumman Corporation

Chris Read – BAE Australia

Andrew Giulinn – Saab Australia

Terry Miles – RUAG Australia

Special thanks goes to Ms Janice Nand (Sparke Helmore Lawyers) for input in relation to Dual/Third Country Nationals and also to Mr Jason Brown (Thales Australia) for his input in relation to Supply Chain Security.

The Group would like to acknowledge the assistance from relevant government agencies (including the Defence Export Control Branch) in the development and review of the Guide.

TABLE OF CONTENTS

INTRODUCTION

The Export Control Forum's Best Practices Working Group, which consist of several Australian Defence Contractors and Government stakeholders, created this guide with the intent that it will serve as a resource to Primes, Small and Medium Enterprises (SMEs), and universities and researchers, in the understanding of their obligations and the development of export compliance programs.

This guide addresses transactions that are outside the scope of the Australia U.S. Defence Trade Cooperation Treaty's 'Approved Community' Arrangements.

Part 1 • **General Information**

Part 1 of this guide provides Australian exporters and universities general information about managing export controlled goods and technology.

Part 2 • **Embargoes, Sanctions and Treaties**

Part 2 of this guide provides an overview of the U.S. Office of Foreign Assets Control (OFAC), the Australia-U.S. Defence Trade Cooperation Treaty (the Treaty) and corresponding screening practices

Part 3 • **Australian Export / ImportControls**

Part 3 an overview of Defence Export Controls (DEC) and Australian Border Force (ABF), and the consequences of violating export control legislation,

Part 4 • **US Export Controls**

Part 4 an overview of International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) including the U.S. Export Control Reform and the consequences of violating export control legislation,

Part 5 • **Australian Best Practice**

Part 5 provides examples of 'for managing controlled exports and technology. It was developed through interviews and the solicitation of written submissions from compliance managers at Australian Defence Contractors.

Part 6 • **Useful Resources**

While the Working Group recognises that resource constraints may make it difficult for SMEs and universities to implement complex compliance programs, we trust that Part 5 of this Guide will help to provide guidance on the essential elements of effective compliance programs, which can be scaled to suit a variety of budgets and resource constraints.

Many Australian exporters in the defence industry manage controlled technology that may also be subject to U.S. export controls, which have extraterritorial reach. As such, we have included in this guide, basic information about the International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR) and Office of Foreign Assets Control (OFAC) as well as best practice materials to assist Australian exporters, particularly SME's, with compliance.

PART 1

General Information about Controlled Exports / Technology

1. GENERAL INFORMATION

1.1. What are export controls?

1.1.1. Australia

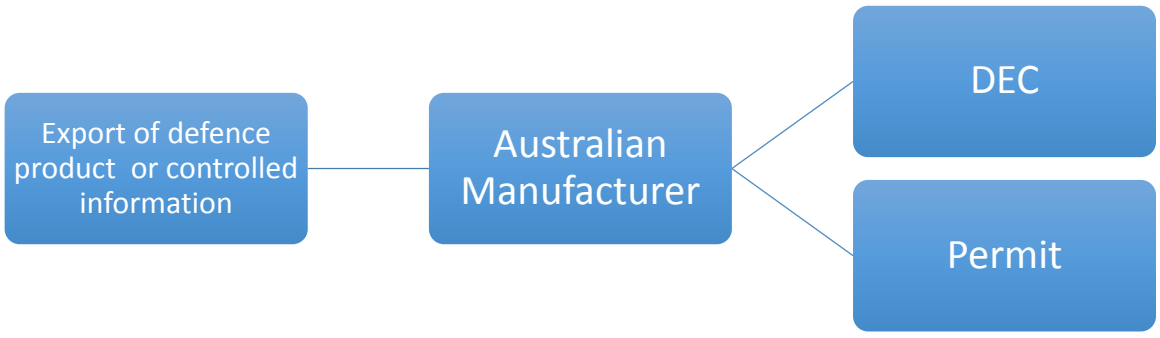
Export control laws regulate the export from Australia to a place outside of Australia for defence and strategic goods and technology including the transmission of certain controlled information.

Exports can be more than physical overseas shipments of defence and strategic goods and technology. Exports can be ‘tangible’ or ‘intangible’.

In the case of ‘tangible exports', items in physical form can be exported by ship, aircraft, post or courier, or by carrying them in checked-in or hand-carried luggage. A ‘tangible export' can include technology stored on a physical medium such as a CD, DVD, USB or computer hard drive or be in the form of blueprints, diagrams or notes.

An ‘intangible export’ (or supply) occurs when a person in Australia supplies or provides to a person located outside Australia with access to defence and strategic technology by electronic means by email, fax, telephone, video conferencing, or providing access to electronic files.

The following figure shows the relationship between an Australian Manufacturer and Exporting product. The manufactures requires a Permit from DEC to enable the export of controlled defence and/or strategic goods or to supply controlled technology and software intangibly.



1.1.2. United States (U.S.)

The U.S. controls all exports from its territory, the movement of certain U.S. origin goods and technology located outside of the U.S., and the intangible export of certain U.S.-origin technology. Exports of U.S. origin military goods and technology, as well as goods and technology that have a 'dual use' and could be used in military or civilian applications, will in most cases, require an export licence from the U.S. government.

U.S. controlled technology in your entity's possession may be listed in a variety of agreements or export licenses or other supporting documents that are noted separately in the relevant annexes. You need to be aware of what you hold in your organisation.

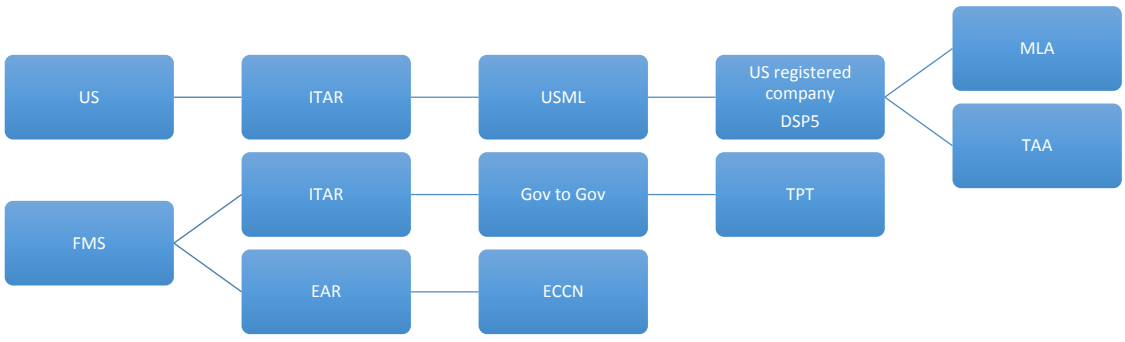
It is important to correctly identify and mark U.S. controlled technology so that appropriate company procedures can be created to safeguard the technology, comply with licence conditions, and maintain required records of 'exports' involving U.S. controlled technology refer table below.

For organisations in Australia the Export Controls apply to re-export and re-transfer of controlled technology.

Re-Exports/ Re-transfers[1]

- Procedures utilised to (a) obtain written State Department approval prior to the retransfer to a party not included in a State Department authorisation of an item/technical data transferred or exported originally to the company, and (b) track the re-export or re-transfer (including placing parties on notice that the proposed transfers involve US origin products and labelling such products appropriately).

The following figure shows the relationship between an Australian Manufacturer and a US registered company holding a DSP5 for approved exports. The Australian manufacturer needs to be listed on an agreement in order to be approved for re-export and/or re-transfer of controlled technology.



[1] The terms "re-export" and "retransfer" are defined in the ITAR and EAR.

1.2. Why is Export Control Important?

In order to prevent sensitive military and dual use technology from being exported to certain countries/end-users where it is feared they may be used for activities that contradict the national interests of the country in which they were developed, controls are placed on their 'export' by many governments around the world. In this Guide, we focus on Australian and U.S. export controls.

Australia and the organisations in Australia that are involved in importing and/or exporting controlled technology, seek to meet a range of important obligations and responsibilities related to export controls including;

1. Compliance with national and international export laws and regulations,
2. Controlling the export, transfer, re-transfer, and re-export of defence or dual-use items to reduce proliferation,
3. Supporting strategic and national interest in non-proliferation,
4. Supporting the Australian Government as an active member of major international arms treaties & multilateral export control regimes,
5. Engaging effectively in multilateral arms control treaties including the:
    a. Nuclear Non-Proliferation Treaty
    b. Chemical Weapons Convention
    c. Biological Weapons Convention
    d. Arms Trade Treaty
6. Participating in multilateral export control regimes including the:
    a. Australia Group
    b. Nuclear Suppliers Group
    c. Missile Technology Control Regime
    d. Wassenaar Arrangement
    e. The Zangger Committee
7. Reducing the risk of legitimate trade being exploited for nefarious purposes, and
8. Being a good corporate citizen by ensuring good governance and ethical behaviour.

1.3. Who should be Concerned about Export Controls?

Big or small, a business entity dealing with Controlled Technology must comply with export controls, or risk penalties such as those described later in this document, which can have very serious consequences. At an organisation level, export controls are a concern for everyone. Adherence to corporate export control policies and procedures is incumbent upon every member of an organisation's staff, permanent or temporary, and in particular, those who have export management and/or export compliance responsibilities.

At an individual level, responsible stakeholders within a business may include managers and staff within the Marketing & Sales, System / Product Development, Accounting, Procurement, Legal, Program / Contract Management, Production, Customer Support,

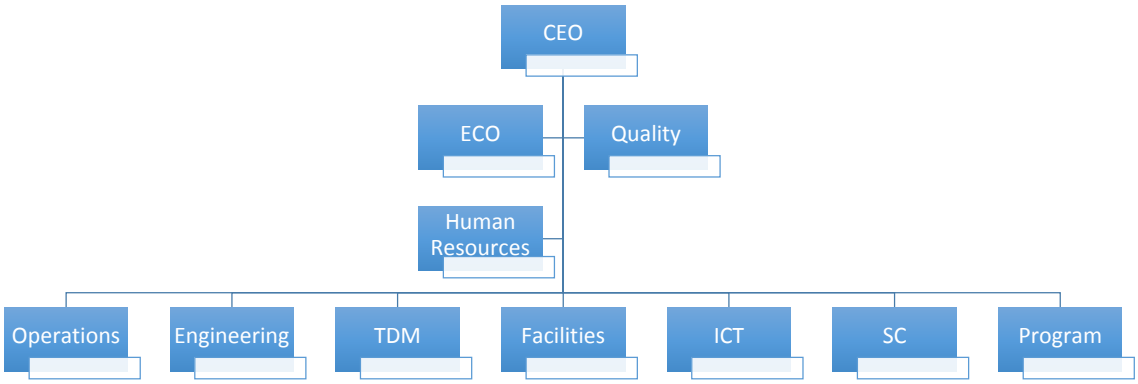
Logistics and Shipping departments. In a smaller organisation, these roles may be combined into a small number of individuals.

Typically an organisation chart identifies most all positions that come into contact with controlled technology at some time during a program and these positions need to be authorised per program, to gain access to controlled technology, according to the approvals given by DEC, and/or U.S. State Department.

The following organisation chart identifies specific roles that may come into contact with controlled technology and/or controlled technical data. In addition the organisation should consider managing access controls for the end user, OEM or customer.

Refer U.S. Getting Started with Defense Trade

http://pmddtc.state.gov/documents/ddtc_getting_started.pdf



1.4. Export Controls: Universities and Research Institutions

While research or teaching work may not be specifically related to weapons or defence, it may involve controlled defence and strategic (dual-use) goods and technology. Export or supply of these items from Australia to a place outside Australia either tangibly or intangibly will require a permit.

The Australian definition (from the DSGL) for “basic scientific research” means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

Also controls on “technology” transfer do not apply to information “in the public domain”, to “basic scientific research” or to the minimum necessary information for patent applications. To further explain the following presents the U.S. view which is quite extensive.

The ITAR defines fundamental research in a bullet under "Public domain means information which is published and which is generally accessible or available to the public" (§120.11).

Further, specifically exempted from the definition of technical data is ... information that is in the "public domain" if published and generally available and accessible to the public through, for example, sales at newsstands and bookstores, subscriptions, second class mail, and libraries open to the public (22 CFR 120.11). Information is also in the public domain if it is made generally available to the public "through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public in the United States" or "through fundamental research in science and engineering at accredited institutions of higher learning in the U.S., where the resulting information is ordinarily published and shared broadly in the scientific community." 22 CFR 120.11(6), (8) [Dept. of State Public Notice 3954]

"Fundamental research means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." ... No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable Further, specifically exempted from the definition of technical data is ... information that is in the "public domain" if published and generally available and accessible to the public through, for example, sales at newsstands and bookstores, subscriptions, second class mail, and libraries open to the public (22 CFR 120.11). Information is also in the public domain if it is made generally available to the public "through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public in the United States" or "through fundamental research in science and engineering at accredited institutions of higher learning in the U.S., where the resulting information is ordinarily published and shared broadly in the scientific community." 22 CFR 120.11(6).

Regardless of the entity or activity, if controlled technology is involved there is an obligation on the part of the entity to abide by the legislation that applies to exports and management of the controlled technology. Therefore, even if an organisation is exporting for research purposes only and even if they are not consciously or purposely working in the defence industry, export controls need to be considered and complied with.

Non-compliance with export controls can have very serious consequences for universities and research institutions. At an individual level, export controls are a concern for all staff and students as well. Adherence to export control policies and procedures is incumbent upon every student and staff member and those with export control responsibilities at the organisation must communicate responsibilities to all affected parties.

1.5. What is or could be a Controlled Export?

'Controlled Technology' is any:

a) physical article or item listed on a control list

b) technical data or technical information listed on a control list or related to a listed item

c) technical assistance/ U.S. “Defense service”, whether provided in person or remotely

d) export controls apply regardless of the state or working condition of the goods or technology.

Controlled technology includes physical items and items such as drawings, blueprints, instructions, photographs, documentation, plans, diagrams, models, manuals, schematics, and any other form of technical data that are the subject of export and import restrictions as to their use and disclosure.

Controlled technology can be stored electronically, recorded onto media or contained in email. Either the Commonwealth of Australia or foreign governments including the U.S. Government impose export controls.

Technology is controlled to reduce global arms proliferation and protect arms technology from misuse by terrorist organisations and countries that are non-signatories to the Wassenaar Arrangements, Missile Technology Control Regime, Australia Group, Nuclear Suppliers Group or arms control treaties.

Note: The terms “defence or dual use technology”, “defence or dual use items”, “defence and strategic goods” and “export controlled products and technology” is used throughout this document to refer to “controlled technology”.

Generally, each Export Control Jurisdiction publishes a list of Controlled Technology relevant to their jurisdiction. A “jurisdiction” may be a single country, such as Australia or the US or a group of countries, such as the European Union.

Australian Controlled technology is listed in the Australian Defence and Strategic Goods List (DSGL), U.S. controlled technology is listed in the ITAR U.S. Munitions List (USML) and the EAR Commerce Control List (CCL). The EU, Japan, and many other countries also have lists enumerating controlled technology. As these countries participate in informal multi-national export control regimes such as the Wassenaar Arrangement and the Australia Group, most countries have similar lists of Controlled Technologies based on the lists produced in these export control forums.

Controlled technologies appearing on control lists include:

i. Military Goods: goods and technologies designed or adapted for use by armed forces or goods that are inherently lethal, such as military goods (those being designed or adapted for military purposes including parts and accessories) and non-military lethal goods (equipment that is inherently lethal, incapacitating or destructive, such as non-military firearms, non-military ammunition and commercial explosives).

ii. Dual-Use Goods: those products developed to meet commercial needs, but which may be used either as components in a military product or system, or in the development or production of military systems or Weapons of Mass Destruction (WMD).

iii. Technologies/Data: any specific information necessary for the development, production, maintenance, repair, modification or use of goods falling under the definitions above, such as instructions, skills, training and working knowledge that is provided in manuals, blueprints, diagrams, or through written and recorded media or devices.

Examples of controlled technology include:

- Complete systems
- Major assemblies, sub-assemblies, component and assemblies, component and piece parts
- Serviceable or unserviceable items
- Technical data, specifications
- Drawings – descriptive, production, modification
- Software – operational, source code, algorithms, etc.
- Production and diagnostic tools and test equipment
- Special materials such as Kevlar, certain metals, etc.
- Information/instructions to operate, maintain, repair, modify the item.

Australia, the U.S. and many other countries with export controls also define the term 'export' as being more than a mere physical shipment across borders. The U.S., for example, considers a telephone conversation where controlled technology is disclosed to a foreign national an "export". In Australia, an export must be extraterritorial but can include such activities as physical exports of tangible products, intangible supply of technical data and providing server access credentials to an overseas party where that server contains DSGL controlled technology. Each export jurisdiction definition of export needs to be examined in order to contextualise what is meant by the term 'export'.

Further, not only is the initial "export" controlled, but many governments also choose to control further "exports" of or future access to the controlled technology. This is referred to as "re-export" or "retransfer" controls.

1.6. Why Australian businesses need to Consider U.S. Export Controls

U.S. export control regulations can essentially affect anyone dealing with U.S. controlled goods or technology. The purchase of U.S. controlled technology compels the purchaser to abide by U.S. export controls, even for foreign items incorporating certain US technology or having a design directly based on U.S. technical data. Furthermore, U.S. export controls (ITAR) apply for the life of the product (even if the classification changes) and a re-export control authorisation must be in place for exports from one non-U.S. country to another, a retransfer authorisation must be in place to provide the controlled technology to an unauthorised entity within the same country and even for the destruction of U.S. origin controlled technology. Thus, U.S. jurisdiction will follow the items, wherever located, and apply to companies with no U.S. ownership.

1.6.1. U.S. Export Controls and Nationality

The U.S. ITAR considers providing controlled technology to a dual national (citizen of one country, born in another) or third country nationals (resident of one country, born in another) to be an export to the country of residence, all countries of citizenship ever held and the country of birth. Therefore, when providing U.S. controlled technology to employees it is essential that nationalities and country of birth be appropriately authorised by the relevant US authority and according to in-house company procedures and policies.

However, it is essential that Australia Anti-discrimination legislation be considered (*an employee cannot be treated less fairly based on their nationality, unless the employer is exempted from Australian state anti-discrimination legislation).

1.7. Non-Compliance Consequences

Both the Australian and U.S. export control regulations (export controls) have a range of penalties for failure to follow their regulatory requirements. The U.S. can prosecute foreign companies for the violation of export controls and may assign severe penalties for violations. Penalties generally relate to the nature and scale of the breach and the intention of the company involved (whether wilful or merely negligent). Severe penalties could be applied in Australia and abroad to companies and individuals within companies found guilty of a criminal offence.

In addition to penalties, consequences of violating export controls can include:

- Placed on one of the U.S. 'denial lists'. As a matter or corporate policy, many U.S. companies will not do business with entities on these lists and, once a company is on such a list, obtaining export permission from U.S. export licensing agencies will become almost impossible. Appearing on a denial list will likely prevent the party from buying U.S. products or technologies.
- Current contracts and those under negotiation might be potentially threatened and access to certain government contracts would be denied. The commercial damage resulting from loss of key contracts and brand devaluation (reputation) in the public eye can be significant.

Penalties for non-compliance with Export Controls can include severe civil and criminal penalties applied against individuals and organisations for violations of the Australian and U.S. export laws and regulations: refer Part 3 and Part 4.

The following penalties can be applied for violations:

- Civil penalties and fines
- Imprisonment
- Denial of export privileges
- Debarment from participating directly or indirectly in the export of controlled technology

Non-compliance with export controls, can cost both the company and the responsible individuals with monetary penalties, as well as imprisonment where breaches were deemed wilful, furthermore export violations can also cause serious reputational harm for the organisation.

To view a list of companies that have been fined by US State Department, refer:

http://www.pmddtc.state.gov/compliance/poa.html

PART 2

Embargoes, Sanctions and Treaties

2. Introduction

Embargoes and sanctions are imposed on subject countries by both the United Nations Security Council and separately by UN member countries as an alternative to armed force. Australia implements United Nations Security Council (UNSC) sanctions regimes and Australian autonomous sanctions regimes as a matter of international law and under Australian sanction laws.

The Australian Government implements Australian autonomous sanctions regimes as a matter of Australian foreign policy. Australian autonomous sanctions regimes may supplement UNSC sanctions regimes, or be separate from them.

The U.S. is at the forefront of imposing sanctions and embargoes on subject countries and this has a huge effect on trade involving controlled technology. Care must be taken when dealing with U.S. controlled technology.

2.1. Australian Sanctions

A number of goods on the Australian Defence and Strategic Goods List (DSGL) are subject to special export restrictions or prohibitions when intended for export to, or end use in, or by countries, individuals and entities subject to United Nations Security Council sanctions or Australian Autonomous Sanctions. For export to countries subject to United Nations Security Council sanctions an export approval from DEC, as well as a separate permit from the Department of Foreign Affairs and Trade (DFAT) is required. The DFAT permit should be sought first. Sanctions change on a regular basis so ensure you check the Australian website regularly.

In addition to the United Nations Security Council sanctions, Australia also implements autonomous sanctions on some countries. Exports of some types of goods to these countries will not be approved. If you are exporting other goods on the DSGL to these countries, you require an export approval from DEC. DEC will consult with DFAT during its assessment of an application to export any goods to these destinations. Current (2016) Australian Autonomous Sanctions include:

- The Former Federal Republic of Yugoslavia
- Myanmar
- Russia/ Ukraine
- Syria
- Zimbabwe

www.dfat.gov.au/international-relations/security/sanctions/Pages/sanctions.aspx

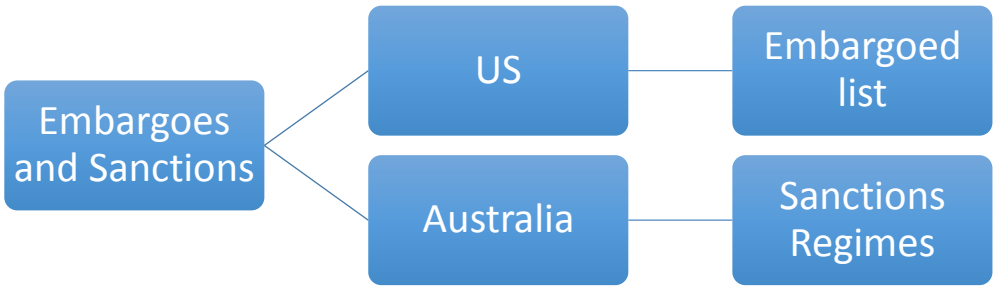
2.2. U.S. Sanctions and Embargoes

The U.S. Office of Foreign Assets Control (OFAC) administers economic sanctions and embargo programs against specific foreign countries or groups to further U.S. foreign policy and national security objectives. In administering these programs, OFAC generally relies

upon Presidential authority contained in the Trading with the Enemy Act (TWEA) or the International Emergency Economic Powers Act (IEEPA), or upon specific legislation, to prohibit or regulate commercial or financial transactions with specific foreign countries or groups.

Examples of current TWEA programs include comprehensive asset freezes and trade embargoes against North Korea and Cuba. Examples of current IEEPA programs include similarly broad sanctions against Libya, Iraq, the Cali Cartel, and certain foreign terrorist groups, as well as comprehensive trade sanctions against Iran.

From time to time, the U.S. Congress has imposed sanctions directly through legislation. Between 1986 and 1991, for example, OFAC administered the trade and investment prohibitions against South Africa mandated by the Comprehensive Anti-Apartheid Act. Similarly, OFAC has been delegated administration of Section 321 of the Antiterrorism and Effective Death Penalty Act of 1996 (the Act), which was signed into law by the President on April 24, 1996



For U.S. Embargoed countries refer to:

http://www.pmddtc.state.gov/embargoed_countries/index.html

2.3. Australian Consolidated List

The Consolidated List includes all persons and entities to which the Charter of the United Nations Act 1945 and the Autonomous Sanctions Act 2011 currently applies. This follows the transition of Australia's targeted financial sanctions from the Banking (Foreign Exchange) Regulations 1959 to the Autonomous Sanctions Regulations 2011. The Australian Consolidated List is also published on the Department of Foreign Affairs website.

The Minister for Foreign Affairs or the Minister's delegate may be able to grant a permit authorising an activity that would otherwise contravene an Australian sanction law. You can contact DFAT in relation to sanctions permits by registering as a user of the Online Sanctions Administration System (OSAS).

http://dfat.gov.au/international-relations/security/sanctions/Pages/online-sanctions-administration-system.aspx

2.3.1. Third Party Screening

Both Australian and U.S. regulations expect that your organisation will actively avoid transactions with sanctioned, embargoed, debarred or otherwise ineligible third parties. Sanctions and embargoes are imposed by the United Nations (UN), the European Union (EU), and individual countries including the United Kingdom, United States and Australia. Sanctions and embargoes may be targeted at individuals, entities, groups, institutions or countries, and are typically intended to achieve specific national security, foreign policy or peace and stability objectives.

For U.S. debarred list refer to: http://www.pmddtc.state.gov/compliance/debar_intro.html

The organisation should:

- Establish a method for the conduct of Third Party Screening. Commercial "Screening Tools" are available. Alternatively, the organisation can directly examine the following sites:
    - United States: http://export.gov/ecr/eg_main_023148.asp and https://www.sam.gov/index.html/#1
    - United Kingdom: https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions
    - Australia: http://dfat.gov.au/international-relations/security/sanctions/pages/sanctions.aspx
- Screening might be performed centrally within the organisation, by a person trained in the selected method. Initiation of screening, however, may be distributed throughout the organisation. Division of responsibility for initiation might logically be:
    - Employees and contract labour – Human Resources.
    - Supply Chain partners – Procurement and contract managers. If the organisation, as part of its Quality Management System (QMS), maintains an Approved Supplier List, consider integrating the screening requirements into the existing qualification process.
    - Parties to teaming and collaborative arrangements – the organisation's Business Development team
    - Customers – to the extent not captured above – contract managers.
- Performing screening centrally allows a single register of screened parties to be maintained and be accessible to other elements of an Export Compliance Management Program (ECMP), as required (the *Employment, Training and Access*, the *Outbound Controls* and *Licencing* elements of the ECMP). A central register also avoids duplication of effort – any initiator should be able to examine the register to determine if screening of their target has already been conducted by others.

3. AUSTRALIAN / U.S. DEFENCE TRADE CO-OPERATION TREATY

In 2007, the Australian and the United States Governments signed the Treaty between the Government of Australia and the Government of the United States of America concerning Defence Trade Cooperation (the Treaty). The Treaty is intended to improve the efficiency of eligible two way transfers between Australia and the U.S. by facilitating the export of

controlled goods, required for certain activities, without the need for an export licence. It is an exemption to ITAR requirements for certain Defence Articles ('Treaty Articles') and certain Government and Non-Government entities. This is achieved through the creation of an Approved Community in Australia and the U.S. which includes government and private facilities.

Refer to: http://www.defence.gov.au/ustradetreaty/

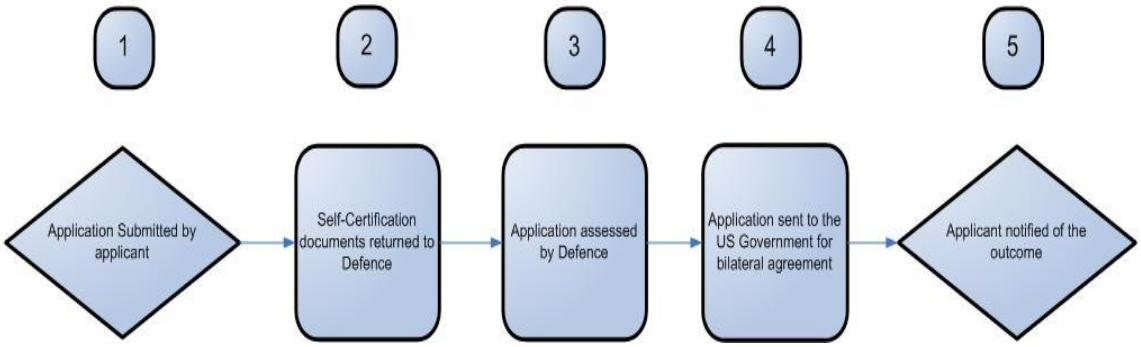
3.1. Approved Community

The Treaty creates an Approved Community (AC) in Australia and the U.S. to enable members to transfer Treaty Articles without the need for separate export licences. Both communities include government and non-government entities that are approved as members of the Approved Community. The Australian Community is managed by the U.S. Trade Treaty Section within DEC. The U.S. Community is managed through the Directorate of Defense Trade Controls (DDTC) within the Department of State.

Australian defence industry or research and education institutions, may apply for Australian Community membership, however, to be eligible the applicant must be a body corporate. Furthermore, there must be either involvement in an approved project / collaboration or an intention to do so to be eligible to apply for membership.

To apply for membership, the following process occurs. For more information, see the Treaty Office website at http://www.defence.gov.au/ustradetreaty/AustralianCommunity.asp

Steps in the Australian Community Application Process



Defence will assess applications to join the Australian Community against the following criteria:

- the organisation's export compliance history under the Australian and U.S. 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;
- 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.

3.1.1. ***Security:*** Australian Community members must ensure that all facilities and Information and Communication Technology (ICT) systems intended for the storage, handling and manufacturing of Treaty Articles have been accredited by Defence. If access is required to classified Articles, the Community Member is required to join the Defence Industry Security Program (DISP) (see: http://www.defence.gov.au/DSVS/resources/DSM/PUBLIC%20DSM%20Part%202.42.pdf)

3.1.2. ***Personnel Security:*** Australian Community Member personnel who require access to Treaty Articles must be Australian citizens with a minimum security clearance of Baseline. The citizenship requirement may be waived on application if a foreign security clearance is held, but this is only with agreement of both the Australian and U.S. Governments.

Refer: http://www.defence.gov.au/ustradetreaty/AustralianCommunity.asp

3.2. Operating under the Treaty

Australian Community Members will be assigned an Australian Community Identification (ACID) number. This ACID number is required for validation of their membership of the Community and should be provided when requested by other Community Members.

3.2.1. Export

Export permission (From Defence Export Control) is not required for the export of Treaty Articles to U.S. 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.

See the current Customs (Prohibited Imports) Regulations, Regulation 3F.

https://www.legislation.gov.au/Details/F2016C00585

3.2.2. Import

Where a Treaty item is listed within Schedule 13 of the Customs (Prohibited Import) Regulations 1956, the requirements for import, as detailed by the Department of Immigration and Border Protection, must be followed. (see: www.border.gov.au/Busi/Impo/Proh/Firearms-and-weapons/official-purposes-test)

3.2.3. Transfers

Transfers under the Treaty can only be made between members of the Approved Community. The recipient is to be confirmed as an Approved Community Member before the transfer takes place.

3.2.4. Transport

To transport a Treaty article, only an approved intermediate consignee must be used. A list of these intermediate consignees can be found on the Treaty website at:

http://www.defence.gov.au/ustradetreaty/Resources.asp

Note that these freight forwarders and couriers cannot be used to transport articles under ITAR arrangements.

3.2.5. Handling and Storage

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 Defence Security and Vetting Service (DS&VS). Link is below.

http://www.defence.gov.au/DSVS/resources/DSM/PUBLIC%20DSM%20Part%202.42.pdf

Any Treaty Article classified by the U.S. is automatically accorded an equivalent Australian security classification and therefore subject to the same protection requirements as an Australian classified Treaty Article.

The Treaty requires that the Australian Government accredits non-government facilities ICT systems used to either access or store Treaty Articles.

Australian Community 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.

Treaty articles must be physically separated from ITAR articles due to the differing access requirements for each even if they are exactly the same article.

3.3. The scope of the Treaty is determined by several elements:

3.3.1. Treaty Articles

The particular articles (good, technology or service must be listed in Part 1 of the Defense Trade Cooperation Munitions List (DTCML). Part 2 of the DTCML lists those articles currently excluded from movement under the Treaty. For articles listed in Part 2, normal licence authorisations will be required for supply and access.

3.3.2. Activities

Four scope lists define the activities under which Treaty arrangements can be used to transfer defence articles:

a) Australian Government End-Use

b) Cooperative Programs

c) Combined Operations and Exercises

d) US Government End-Use projects (projects related to security or defence where the US Government is the end-user).

These end-use lists as well as other information can be viewed at:

http://www.defence.gov.au/ustradetreaty/resources.asp

In summary, to be able to use the Treaty, the entity must:

- Be a member of the Australian Community
    - Meet physical, ICT and citizenship requirements; AND
- Be involved in or intend to be involved in an approved project/program/activity
    - The technology must be listed in Part 1 of the DTCML.

3.4. Reference

Defence has provided an Australian-US Defence Trade Cooperation Treaty Manual that provides additional information and detail. The manual can be accessed at:

http://www.defence.gov.au/ustradetreaty/pdf-docs/AC-Manual-Nov16.pdf

PART 3

Australian Controls

4. OVERVIEW OF AUSTRALIAN EXPORT CONTROLS

The **Defence and Strategic Goods List (DSGL)** specifies Australian controlled technology that requires an export permit or licence from DEC prior to the tangible export or intangible supply of technology listed on the DSGL. The DSGL includes equipment, assemblies, components, test equipment, software and technology and consists of two parts. Part 1 of the DSGL contains the munitions list, which includes both military goods and non-military lethal goods. Part 2 of the DSGL comprises a list of dual use goods and technologies that were developed to meet commercial needs but also have application in a military system or in a Weapons of Mass Destruction (WMD) program.

The Department of Defence is responsible for administering Australia's exports approvals for defence and strategic goods. The Minister for Defence has delegated the authority to issue export licences to the Defence Export Control Branch (DEC), within the Department of Defence. DEC is responsible for assessing export licence applications and granting export permits and licences.

The Department of Immigration and Border Protection ("Customs") is responsible for the enforcement of export controls, including verifying that the required permits and licences are in place prior to export or import, and for monitoring compliance with Australian export controls. Customs has the power to conduct audits and is the agency that handles disclosures of export violations.

4.1. Legislative Basis for Australian Export Controls

The **Customs Act 1901** and **Regulation 13E of the Customs (Prohibited Exports) Regulations 1958** (PE Regs) control the tangible export of defence and dual use goods in Australia. Regulation 13E prohibits DSGL listed goods from being physically exported from Australia without a licence or permit. While a permit is not required for technology not listed on the DSGL, it is recommended that exporters should undertake due diligence in any foreign trade to ensure the legitimacy of any export.

The Customs Act 1901 now includes a military "catch-all" military end-use provision whereby the Minister for Defence may deny the export of a non-controlled good to a suspected military end-use. If an exporter suspects the export may be for a military end-use that might be contrary to Australia's defence, security or international relations, they should contact DEC for advice and assistance.

The **Weapons of Mass Destruction (Prevention of Proliferation) Act 1995** provides for the control of exports of non-controlled goods or the supply of services or technology where there is a belief or suspicion that the export or supply may be used in, or assists a WMD program. This is a "catch-all" legislation and has no "control list".

The **Charter of the United Nations Act 1945** implements UN sanctions, which include arms embargoes, bans on import and export of certain commodities, travel restrictions, financial sanctions, and the suspension of diplomatic ties. The responsibility for administering Australia's commitment to UN sanctions, as well as Australia's autonomous

sanctions under the **Autonomous Sanctions Act 2011** lies with the Department of Foreign Affairs and Trade (DFAT). Australian exporters should be familiar with sanctions and ensure effective screening is in place to prevent violation of sanctions laws.

The **Defence Trade Controls Act 2012** implements the Australia-U.S. Defence Cooperation Treaty (the Treaty) and regulates the intangible supply of controlled technologies on the DSGL. This includes the supply of technology by electronic means. The Act also regulates brokering the supply of DSGL goods and technology and publishing controlled technology. Guidance on the strengthened export controls, including brokering and publishing controls can be found on the DEC website (http://www.defence.gov.au/ExportControls/SEC.asp).

The Act was amended in 2015 to take account of concerns from the universities and research sector.

The **Defence Trade Control Regulation 2013** outlines the requirements for becoming an Approved Community member under the Treaty. Though the aforementioned Acts and Regulations constitute the main body of export controls in Australia, many pieces of Australian legislation interact with these Acts and Regulations.

4.2. Who Administers Australian Export Controls?

Most Australian exporters of controlled goods and technologies will need to interact with the following key government agencies when planning the shipment, delivery or transmission of controlled items:

- **Department of Defence**
    - **Defence Export Control Branch (previously DECO, now DEC)** regulates the export, supply and brokering of defence and dual-use goods and technologies as part of the Australian export control regime, and issues export licences and/or permits where required.
    - Information and further guidance about the process of applying to DEC for an export licence or permit can be found on the DEC website:

      http://www.defence.gov.au/ExportControls/Default.asp

    - **U.S. Trade Treaty Section** within DEC manages the Treaty, the Australian Community and the defence trade of eligible and approved items between Australia and the United States only (Note: it is different from regular trade of U.S. controlled items under ITAR and EAR).
- **Department of Immigration and Border Protection (Customs)**
    - Facilitates legitimate trade
    - Regulates trade and movement of people across Australian borders.
    - Verifies that export and import permits have been obtained prior to the cross border movement of controlled goods
    - Has monitoring powers
    - Responsible for enforcement and compliance
    - Issues import permits for war-like goods, where required

- **Department of Foreign Affairs and Trade**
    - Formulates trade policy
    - Represents Australia internationally at export control regimes
    - Implements sanctions (including the provision of permits), which restrict the export of certain goods to particular countries or designated individuals and entities.
- **Australian Federal Police**
    - Investigation and prosecution powers.

4.3. How to Export Australian Controlled (DSGL) Technology?

The first step to exporting or supplying DSGL controlled technology is to register with DEC as a client. It is also important to register before conducting any brokering activities. To register as a DEC client you must submit a Client Registration Form to DEC:

http://www.defence.gov.au/ExportControls/Register.asp

If you are unsure whether your technology is listed on the DSGL, you may use the Online DSGL tool to assist you to establish whether or not you will require a permit from DEC to export, supply, publish or broker your goods, software or technology. The Online DSGL Tool will also help you determine whether you are conducting a controlled activity (i.e. exporting, supplying, publishing or brokering):

https://dsgl.defence.gov.au/Pages/Home.aspx

If you are unable to determine whether your goods or technology are controlled you may seek a formal assessment from DEC after registering as a client and then submitting an Application for DSGL Assessment:

http://www.defence.gov.au/ExportControls/FormDSGLAssess.asp

Once it has been determined that your good or technology is controlled, you will need a permit/licence to export, supply, publish or broker it.

The application process with DEC primarily requires submitting a specific form:

- If exporting or supplying a technology (both tangible and intangible), you must submit a completed Application to Export or Supply Controlled Goods or Technology form.
- If brokering a supply of a controlled good or technology, you must submit a completed Application to Make a Brokering Arrangement form to DEC (Note: The Applicant must be a Registered Broker with DEC before submitting this application).
- Publication controls only apply to Part 1 (Military) DSGL technology. The publication of Part 2 (Dual-Use List) DSGL technology is not regulated; no approval is required from Defence. If planning to publish any Part 1 DSGL Technology, you must contact DEC directly.

All application forms are available from the Forms page on the DEC website: http://www.defence.gov.au/ExportControls/Forms.asp

Some licences and permits are issued with conditions that may require that the exporter provide information to DEC. All reporting conditions are explained in the licence or permission provided by DEC.

More information on the export application process can be found at the DEC website (http://www.defence.gov.au/ExportControls/ApplicationProcess.asp)

Exporters may also seek an "In-Principle" assessment to export controlled items. To seek in-principle assessment you submit a completed "Application to Export or Supply Controlled Goods or Technology" and indicate in the form that the application is for in-principle assessment. This provides a preliminary advice to the exporter, which indicates the likely outcome of the future application to export a controlled item to a specific destination or end-user. **This is not an export approval**.

4.4. Export permits

There are a number of different types of export permits available for both military and dual use goods. These include single use permits, permits issued for a period of up to five years, permits issued for the life of a project and multiple-use permits for the export or supply of certain Part 2 DSGL goods to certain approved destinations.

4.4.1. Physical (tangible) export permits

A permit is required to export defence and strategic goods and technology in physical form such as by sending them by ship, aircraft, post or courier or by carrying them in checked-in or hand-held luggage. Physical exports can be in the form of technology or software stored on a physical medium such as a CD, DVD, USB or computer hard drive or blueprints, diagrams or notes.

4.4.2. Supply (intangible) permits

A permit will be required when a person in Australia supplies DSGL technology in an electronic or other intangible form to a person located outside Australia. This includes providing access to DSGL technology (for example by providing passwords to access electronic files stored on a database located in Australia).

Exceptions

- A permit is not required for publication supply of Part 2 DSGL technology.
- A permit is not required for oral supply of DSGL technology (for example telephone conversations, video conferences, live streaming or webinars) UNLESS

(i) the oral supply is for the purpose of providing a person with access to DSGL technology (for example providing a password to a data base located in Australia containing DSGL technology) OR

(ii) the oral supply is for the purpose of providing the DSGL technology for use in a Weapons of Mass Destruction program or for a military end-use.

4.4.3. Publication approvals

An approval will be required to place Part 1 DSGL technology in the public domain by publishing it on the internet or otherwise. This requirement applies to anyone located in Australia or an Australian citizen or resident located outside Australia.

Exception

A publication approval is not required for publication of Part 2 DSGL technology.

4.4.4. Brokering permits

A brokering permit will be required where a person acts as an agent or intermediary to arrange the transfer of Part 1 defence and strategic goods and technology between 2 places located outside Australia AND receives money or a non-cash benefit or advances a political, religious or ideological cause. Note: a person must be registered as a broker before a brokering permit can be applied for.

Exceptions

1) A permit is not required for brokering the transfer of defence and strategic goods and technology from a listed country – the country list is a legislative document and is available here: https://www.legislation.gov.au/Series/F2016L00548 .
2) A permit is not required for brokering Part 2 defence and strategic goods and technology unless the Part 2 defence and strategic goods and technology are being brokered for a military end-use or a Weapons of Mass Destruction program.

Further information on registering as a broker and applying for a brokering arrangement permit is available on the DEC website:
http://www.defence.gov.au/ExportControls/Brokering.asp

4.4.5. Multi-party (project) permits

An application can be made by a single applicant (for example the University) working on a joint project or collaborative activity, on behalf of all the other parties who will require an export permit.

If DEC assesses that the applicant and co-applicants may have a permit, it will contact each co-applicant and confirm their need for a permit. Once approved, the applicant and the co-applicants will each be issued a permit with identical descriptions of the approved items, consignees and end-users. However, each permit will only list one permit holder and will be uniquely numbered.

DEC can amend issued permits and additional collaborators can be added to all permits by application by the original applicant (depending on DEC's assessment).

4.4.6. Permit Applications

DEC has stated its preference for organisations to have a single DEC Client Registration Number (DCRN) and designated representative to allow ease of communication between DEC and the organisation.

4.4.7. Recordkeeping

Records of physical exports of defence and strategic goods and technology and intangible supplies of DSGL technology made under permits must be kept for a period of 5 years from the date of export or supply.

4.4.8. Australian General Export Licences (AUSGELs)

As an alternative to normal permits, and only for qualifying circumstances, DEC provides AUSGELs.

These licences are broad permits for pre-approved goods to pre-approved destinations and purposes for five years duration, or longer if required. The exporter submits the 'Application for an Australian General Export Licence' form. Once approved, you can export any of the listed controlled items to any of the approved destinations if it matches the approved purpose of export listed in the AUSGEL.

DEC will only issue AUSGEL to applicants who are likely to use the licence for its intended purpose and comply with the conditions stated on the licence. AUSGELs also have some additional reporting requirements.

AUSGEL are issued for the following purposes:

1. AUSGEL 1: Licence for the Export of Certain Dual-use Goods to Specified Destinations. Licence for the Supply of Certain DSGL Software and Technology to Specified Destinations
2. AUSGEL 2: Licence for the Export of Certain Dual-use Goods to Specified Destinations for Repair or Return
3. AUSGEL 3: Licence for the Export of Certain Military Goods to Specified Destinations for Repair or Return
4. AUSGEL 4: Licence for the Export of Certain Military Goods to Members of the Federal, State or Territory Police, Australian Public Service, Australian Defence Force and Australian Intelligence Community.
5. AUSGEL 5: Licence for the Export of Certain Dual-use Goods to Members of the Federal, State or Territory Police, Australian Public Service, Australian Defence Force and Australian Intelligence Community.

4.4.9. The current (2016) approved AUSGEL destinations:

Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, United Kingdom and the United States.

4.5. Australian Penalties

Australia takes non-compliance with export controls very seriously. Below is a chart outlining the penalties that an individual or entity may incur because of violating Australian legislation: Fines are based on Penalty Units, which are defined in section 4AA of the Crimes Act 1914 and are currently valued at one Penalty Unit is $180 for a Federal offence (Penalty Units are reviewed every three years. The next review is due on 1 July 2018).

	Customs Act 1901 *	Sanctions under the Customs Act	Weapons of Mass Destruction Act 1995	Criminal Code Act 1995 (for false/misleading statements and misrepresentation of facts)	Defence Trade Controls Act 2012 **
Individual	Up to $A425,000 and/or 10 years imprisonment for individuals	Up to 10 years imprisonment	Up to 8 years imprisonment	2 year of imprisonment and $A12,000 for individual	Up to $A425,000 and/or 10 years imprisonment $A5,100 for inadequate recordkeeping
Company	$A2.125m for a company	—	—	$A60,000 for corporation	

* E.G. exporting DSGL controlled technology without a DEC permit

** E.G. making an intangible supply of DSGL controlled technology without a DEC permit

5. Overview of Australian Import Controls

Within the realm of defence and dual use goods and technology, there are controls on the importation of weapons, weapon parts and weapon systems just to start. Therefore, any attempts to import such items without an appropriate permit will be met with the goods being seized and even confiscated, and possible prosecution.

The **Customs Act 1901** and the **Customs (Prohibited Imports) Regulations 1956 (PI Regs)** controls the import of specified goods into Australia. **Schedule 6 and 13** of the Prohibited Import Regulations details the requirements for the importation of war-like systems, weapons and weapon parts. Generally, dual-use parts do not require an import permit, but should be confirmed with Customs if there is any doubt.

The **Customs (Prohibited Imports) Amendment (Firearms and Other Weapons) Regulation 2015** came into effect on 15 December 2015. This amends the Customs (Prohibited Imports) Regulations 1956 to streamline certain processes for the lawful importation of certain firearms and weapons under specific circumstances.

The major changes to the Prohibited Import Regulations include:

- Import permission will no longer be required for the following:
- Schedule 13 goods imported for the purposes of transhipment (Regulation 3D).
- The re-importation of firearms used in lawful shooting or hunting activities overseas by Australian residents (subject to conditions in new Regulation 3E).
- Eligible Schedule 13 goods imported by Australian Community members of the Australia-United States Defence Trade Cooperation Treaty (new Regulation 3F).

- Military vehicles, aircraft and vessels within the categories of battle tanks, armoured combat vehicles, combat aircraft, attack helicopters and warships are now controlled under new Item 1A of Schedule 13.
    - This ensures that offensive military vehicles, aircraft and vessels that contain weapons are controlled on import. It also ensures that civilian dual-use parts and components, which are unrelated to weapons (such as axles, engine parts, gearboxes, rotors etc.), can be imported without a permit. Weapons, weapons parts and components that can be fitted to any type of vehicle, aircraft and vessel remain controlled under Item 1 of Schedule 13.

As the Prohibited Imports Regulations are regularly updated, it is prudent to check the Federal Register of Legislation website for the most current version and always click the "Go To Latest" link tab at the top right. Refer:

https://www.legislation.gov.au/Details/F2016C00585

A valid import permit must be in place before the controlled goods reach the Australian border. If the permit is not in place:

- Customs may refuse entry of the goods that are being imported holding them up at the border or even requiring return (re-export needing a DEC permit) to its origin;
- Customs may seize those goods temporarily or permanently; and
- All costs related to import delays, re-exports and seizure will be charged to the company.

Concerning defence industry, the most common controlled imports are weapons and explosives. For information that is more specific the Department of Immigration and Border Protection website will provide more information.

www.border.gov.au/Busi/Impo/Proh

6. Australian Trusted Trader

The Australian Trusted Trader (ATT) program is an initiative of the Australian Government Department of Immigration and Border Protection.

Australian Trusted Trader is an Authorised Economic Operator (AEO) program. AEOs work to secure the international supply chain, while facilitating the movement of legitimate trade.

Essentially, the program recognises those organisations that are importers/exporters of product, and specifically provides certain benefits to traders approved under ATT. These benefits include:

- a dedicated **Account Manager** who will be the point of contact between Australian Border Protection and the business
- **priority service** when requesting advanced rulings on tariffs, valuation and origin
- **differentiated examinations** as we would be recognised as low risk
- use of the Australian Trusted Trader logo

For more information refer: http://www.border.gov.au/Busi/Trus

PART 4

U.S. Export Controls

7. OVERVIEW OF U.S. EXPORT CONTROLS

The U.S. controls all exports from its territory, the movement of certain U.S. origin goods and technology located outside of the U.S., and the intangible export of certain U.S.-origin technology. Exports of U.S. origin military goods and technology, as well as goods and technology that have a 'dual use' and could be used in military or civilian applications, will in most cases, require an export licence from the U.S. government. In some cases, it is also required to obtain a licence from the U.S. government before making an export that is intangible in nature. Examples include sending an email that discloses controlled technology or providing access to controlled technology to a 'foreign person'.

U.S. controlled technology in your entity's possession may be listed in a variety of agreements or export licenses or other supporting documents that are noted separately in the relevant annexes. You need to be aware of what you hold in your organisation.

It is important to correctly identify and mark U.S. controlled technology so that appropriate company procedures can be created to safeguard the technology, comply with licence conditions, and maintain required records of 'exports' involving U.S. controlled technology refer table below.

The **Arms Export Control Act (AECA)** is the cornerstone of U.S. law governing the export of military goods and technology. The U.S. Department of State implements the AECA by administering the **International Traffic in Arms Regulations (ITAR)** through their Directorate of Defense Trade Controls (DDTC).

Dual use goods and technology are governed by a different set of laws and regulations. The **Export Administration Act** authorises the Department of Commerce (DoC) to regulate the export of dual-use goods and technology. The **Export Administration Regulations (EAR)** is administered by the DoC Bureau of Industry and Security (BIS).

	Military Goods		**Dual Use**
Type	**Gov to Gov**	**Direct Commercial Sales**	
Agency	Department of Defense (DOD)	Department of State's Directorate of Defense Trade Controls (DDTC)	Department of Commerce's Bureau of Industry and Security (BIS)
Legislation	Foreign Military Sales (FMS), ITAR 126.6c	ITAR	EAR
Handling (e.g. Classification)	Special requirements	USML Category 1…etc	600 Series
			ECCN

7.1. FMS

In many instances, the Australian Government has acquired controlled U.S. defence equipment and technical data via Government-to-Government arrangements, this is known as **Foreign Military Sales (FMS)**. The defence equipment may contain ITAR, EAR and/or non-controlled material, but all must be managed under FMS rules. Under U.S. requirements associated with export control of FMS articles, it is only the Commonwealth (the project) that can apply for a specific Department of State approval (known as a Third Party Retransfer [TPR]) to allow industry access to FMS equipment and technical data. Where additional sub-contractors require access to FMS articles beyond those listed on the original TPR approval, the releasing industry party must approach the Commonwealth (project) sponsor of the TPR to obtain approval to add these additional parties before the transfer can occur. Department of State TPR approvals can take upwards of three months.

7.2. Key U.S. Government Organisations involved in Export Controls

When handling controlled technology that originates from the United States, the Australian company will most likely have to interact with the U.S. supplier who will work with the following two U.S. agencies in order to secure proper authorisations for exporting or transferring. However, direct interaction with U.S. agencies is also possible, and even encouraged for EAR controlled technology:

- **U.S. Department of State – Directorate of Defense Trade Controls (DDTC),** which administers the control of military goods and technologies known as the International Traffic in Arms Regulations (ITAR) and the U.S. Munitions List (USML)

The DDTC will only issue licences to US companies that are registered with the DDTC as manufacturers or exporters of ITAR controlled technology. Only U.S. companies are able to register. Therefore, the only means by which Australian companies can obtain an approval from the DDTC for re-export of an ITAR controlled article are to either ask the U.S. supplier to submit a licence application to the DDTC for the re-export transaction or to send the DDTC a letter (General Correspondence) asking for re-export approval.

- **U.S. Department of Commerce – Bureau of Industry and Security (BIS)**, which administers the control of dual-use goods and technologies known as the Export Administration Regulations (EAR) and the Commerce Control List (CCL). Australian companies are encouraged to approach BIS with queries and make licence applications directly to BIS through the SNAP-R system on the BIS website.
- **The Office of Foreign Assets Control (OFAC)**, administers economic sanctions and embargo programs against specific foreign countries or groups to further U.S. foreign policy and national security objectives. In administering these programs, OFAC generally relies upon Presidential authority contained in the Trading with the Enemy Act (TWEA) or the International Emergency Economic Powers Act (IEEPA), or upon specific legislation, to prohibit or regulate commercial or financial transactions with specific foreign countries or groups.

There are other foreign government agencies that also regulate export controls from which an Australian organisation may be required to seek permission when re-exporting or re-transferring the controlled technology originating from that country.

7.3. U.S. Export Control Reform

In August 2009, President Obama directed a broad-based interagency review of the U.S. export control system with the goal of strengthening national security and the competitiveness of key U.S. manufacturing and technology sectors by focusing on current threats and adapting to the changing economic and technological landscape. Refer:

http://www.pmddtc.state.gov/ECR/index.html

Later in 2013, the U.S. began a systematic review of the ITAR in order to reduce the number of technologies listed on the USML. As part of this Export Control Reform (ECR) process, many ITAR controlled articles were moved to the jurisdiction of the EAR and are now listed on the CCL. As part of ECR, not only have articles transitioned from the USML to the CCL, but the USML has also been completely revised, making pre-reform USML classifications invalid. In some cases, articles will remain under the ITAR, but the revision of the USML will necessitate a review of the article against the revised USML to determine the new USML classification.

It is important and commercially advantageous for Australian industry to understand how their inventory and provision of services was affected by ECR as approval to export EAR controlled items is issued in the form of a licence by another U.S. government agency, the Bureau of Industry and Security. Licences for EAR controlled technology can be obtained by Australian industry directly from BIS and the processing times are on average just three weeks. Further, in many cases, no licence is required for the export of; including providing a foreign person or another Australian company access to, EAR controlled items.

7.3.1. Key Changes Arising from Export Control Reform

- Most, but not all, of the items changing jurisdiction from the ITAR to the EAR will be classified as “600 Series’ items on the CCL. This is to allow them to be easily identified as formerly ITAR controlled. Special rules regarding licensing requirements, exception usage, recordkeeping, and reporting requirements apply to 600 series items.
- Most categories of the ITAR USML have been rewritten and re-organised and new categories created. As a result, USML classifications assigned pre-ECR are now either incomplete or incorrect. All USML classifications will need to be reviewed in the face of the reform and corrected.
- Non-U.S. Companies are authorised to make their own determinations of changes to the jurisdiction and classification of goods and technology post U.S. export control reform. The U.S. exporter and/or OEM are an essential resource for assistance with making these decisions and, where possible, should be consulted during the decision-making process.
- Certain goods and technology that have moved from the USML to the CCL may no longer require a licence or may be eligible for export without a licence under an EAR licence exception. However, the U.S. government will closely monitor the export and

re-export of items under certain exceptions for the next several years, making recordkeeping increasingly important for Australian entities exporting or receiving EAR controlled items under a licence exception.

- Australian entities may apply to the BIS for Commerce Department licences to export, re-export, and retransfer EAR controlled items. Australian entities can apply for both classification advice (Commodity Classification Request) and licences (Re-export licences) through the BIS' on-line portal, SNAP-R. SNAP-R accounts can be opened at no cost and there is no cost for classification advice or licence applications.

The most current version of both the ITAR (Title 22, Part 120-130) and the EAR (Title 15, Part 730 – 774) can be found on the e-CFR website www.ecfr.gov. The eCFR is updated within 48 hours of any legislative changes coming into effect.

Australian companies will be responsible to the BIS for compliance with the EAR. As part of the ECR, the BIS will increase its end-use verification visits abroad, including in Australia, and as such, some of Australia's transactions may be subject to interim reviews by BIS officers.

To ensure compliance with the ITAR and EAR, it is important for Australian compliance officers to understand the classification, licensing, and record keeping requirements of ITAR and EAR. The process of correctly classifying articles making the transition from the jurisdiction of the ITAR to the EAR is an important part of ensuring compliance.

7.3.2. Change of Jurisdiction from ITAR to EAR

It is the responsibility of Australian companies to review U.S. controlled technology in their possession and care to determine whether the ITAR or EAR is currently the correct jurisdiction of the item and the corresponding correct classification.

Steps involved in jurisdiction determination:

- Understand the nature and functionality of the item and have technical resources such as brochure, data sheets, specs, and access to an engineer familiar with the article/item available.
- Review the revised USML (where the current USML classification is available, review the applicable USML category).
- Read through the most recent published changes to the USML with the aim of identifying the article on the enumerated list of controlled items in the applicable category. If the article is not enumerated, but may be described as specially designed for a military purpose or to work with an ITAR controlled article listed on the USML, determine if the article meets the revised ITAR definition of 'Specially Designed'.
- Where the article is neither enumerated nor 'Specially Designed' under the ITAR, the article has transitioned to the EAR CCL.

ECCN are determined based on an item's technical parameters and specifications. It is therefore of paramount importance to understand the nature and function of the items and have access to relevant technical specifications before consulting the CCL to identify an applicable ECCN. Engineers familiar with the item should be consulted where information

cannot be obtained from documentation such as brochures, manuals, Australian Standards, designs, and other reliable sources such as the OEM. The source(s) of the information and reasoning used to determine the ECCN should be documented in a classification matrix should future questions about the item's classification arise. Engineers should be consulted wherever doubt about the functionality of an item exists (i.e. the item is designed to perform a certain function but has the technical ability to surpass that design intent).

U.S. suppliers may be one source for obtaining an item's ECCN. Although most U.S. suppliers are able to provide an ECCN for their products and technology, these ECCN may not always be correct. The Australian company intending to make the export is ultimately responsible for ensuring the correct classification of items subject to the EAR and as such should work to determine the ECCN and confirm the information provided by a supplier. Where a supplier provides an ECCN, the source of the information (name and contact number, website, etc.) should be retained in a classification matrix or other suitable record.

In instances where the provided ECCN does not seem reasonable, the Australian company can choose to determine their own classification. They may also choose to ask the U.S. Bureau of Industry and Security for a classification advice through making a classification request in SNAP-R.

Details about ECCN and the process of classifying can be found in the EAR Annex D.

7.4. US ITAR Requirements

The CFR is the codification of the general and permanent rules of the Executive departments and agencies of the U.S. Federal Government.

The new revised USML Categories are:

I	Firearms, Close Assault Weapons, and Combat Shotguns
II	Guns and Armament
III	Ammunition/Ordnance
IV	Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
V	Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents
VI	Surface Vessels of War and Special Naval Equipment
VII	Ground Vehicles
VIII	Aircraft and Related Articles
IX	Military Training Equipment and Training
X	Personnel Protective Equipment
XI	Military Electronics
XII	Fire Control, Range Finder, Optical and Guidance and Control Equipment
XIII	Materials and Miscellaneous Articles
XIV	Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
XV	Spacecraft and Related Articles
XVI	Nuclear Weapons and Related Articles
XVII	Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
XVIII	Directed Energy Weapons

XIX	Gas Turbine Engines and Associated Equipment
XX	Submersible Vessels and Related Articles
XXI	Articles, Technical Data, and Defense Services Not Otherwise Enumerated

Primary sections of CFR22 to consider in your company Export Control Program.

CFR22 ITAR PART	**Description**
120	Purpose and Definitions
121	USML
122	Registration of U.S. manufacturers and Exporters
123	Licenses for the export of U.S. defense articles
124	Agreements, Off-shore procurement and other Defense services
125	Licenses for the Export of Technical Data and Classified Defense Articles
126	General Policies and Provisions
127	Violations and Penalties
128	Administrative Procedures
129	Registration and Licensing of Brokers
130	Political Contributions, Fees and Commissions

7.5. What is a Deemed Export?

The U.S. considers an export of controlled technology to have taken place when it is released to a non-U.S. person. Examples of deemed exports can include:

1. allowing non-U.S. persons to view or access the controlled technology,
2. sending an email containing controlled technology to a non-U.S. person,
3. communicating controlled technology over the phone, for example in providing technical support or training.

A licence must be obtained granting permission to ‘export’ before these releases can take place as the technology is ‘deemed’ by the U.S. to be exported to the home country of the non-U.S. person.

In Australia, we use the term ‘intangible supply’ to refer to exports of technology that are not physical, such as sending controlled technology over email. The **Defence Trade Controls Act 2012** (DTCA) describes the controls on intangible supplies. The key difference between U.S. deemed exports and Australian intangible supply is that the U.S. regards domestic transfers to foreign persons to be an export, while Australian legislation only applies to transactions that occur between an Australian entity and an entity located outside the physical territory of Australia.

7.6. Destination Control Statement

It is a U.S. requirement that the appropriate Destination Control Statement (Statement) is stated as an integral part of the commercial invoice in accordance with requirements of §758.6 of the EAR and the ITAR §123.9 whenever the item is shipped. The Statement will enable you to identify the jurisdiction of an item.

Each company's level of involvement in exporting, the circumstances under which they trade, and the nature of products and technology they trade will affect the complexity of how their internal compliance program serves to protect export controlled products and technology. Part Two of this guide seeks to provide guidance and examples of export compliance considerations and best practices that may be considered for inclusion in an SME's internal compliance program. The guidance and examples provided herein may or may not apply to your company's circumstances.

The Statement has been harmonised between Departments of Commerce and State and is now common to both. The following statement is current as of 15 November 2016.

> *"These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations".*

7.6.1. Additional requirement for any 9x515 or "600 series" article

In addition to the Statement as required in the above paragraph, the **ECCN** for each 9x515 or "600 Series" item being exported must be printed on the commercial invoice and on other export control documents that accompanies the shipment from its point of origin to the ultimate consignee or end-user abroad.

7.7. Government Programs (Blue Lantern, End Use Verification visits)

The U.S. Government has three main End-Use Monitoring programs:

- Blue Lantern – Direct Commercial Sales (DCS) of United States Munitions List (USML) articles, technology, services, and brokering.
- Golden Sentry - Foreign Military Sales (FMS) of defence articles and services via government-to government channels
- End-Use Checks - Dual-use items and munitions on the Commerce Control List (CCL)

The End-Use Monitoring Programs verifies end-users, consignees, and end-uses of U.S. exports of defence articles, technology, and services. There are approximately 55% pre-licence and 45% of post-shipment checks done annually. These checks are performed worldwide by U.S. Embassy personnel in cooperation with between 80 to 100 host governments since 1990. The benefits of the programs include:

- Increased confidence and cooperation

- Expedites future requests
- Facilitates transfer of more advanced technology
- Helps vet vendors, prevent diversions
- Protects end-users from untrustworthy intermediaries
- Fosters communication among U.S. government, host country, and industry
- Establishes expectation of due diligence by exporters and importers, educates industry on laws and regulations

7.8. Watch List

All U.S. licence applications are checked against the U.S. Government Watch List. The list includes more than 60,000 entities, which is compiled from multiple sources. Any matches may result in a Blue Lantern check. List to check include:

1. **Denied Persons List**: A list of individuals and entities that have been denied export privileges. Any dealings with a party on this list that would violate the terms of its denial order are prohibited.
2. **Unverified List**: A list of parties where BIS has been unable to verify the end use in prior transactions. The presence of a party on this list in a transaction is a "red flag" that should be resolved before proceeding with the transaction.
3. **Entity List**: A list of parties whose presence in a transaction can trigger a licence requirement under the EAR. The list specifies the licence requirements that apply to each listed party. These licence requirements are in addition to any licence requirements imposed on the transaction by other provisions of the EAR.
4. **Specially Designated Nationals List**: A list compiled by the Treasury Department, OFAC. OFAC regulations may prohibit a transaction if a party on this list is involved. In addition, the EAR requires a license for exports or re-exports to any party in any entry on this list that contains any of the suffixes "SDGT". "SDT", "FTO" or "IRAQ2". https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx
5. **Debarred List**: A list compiled by the State Department of parties who are barred by §127.7 of the ITAR from participating directly or indirectly in the export of defence articles, including technical data or in the furnishing of defence services for which a license or approval is required by the ITAR. http://pmddtc.state.gov/compliance/debar.html
6. **Non-proliferation Sanctions**: Several lists compiled by the State Department of parties that have been sanctioned under various statutes. The Federal Register notice imposing sanctions on a party states the sanctions that apply to that party. Some of these sanctioned parties are subject to BIS's license application denial policy described in 744.19 of the EAR.

7.9. Dual and Third Country Nationals

Under U.S. trade controls, issues of nationality combined with any previous citizenship held and country of permanent residency must be considered when determining who can have access to U.S. Export Controlled (ITAR, FMS & EAR) goods, data or services.

However, such considerations may be unlawful under Australian anti-discrimination law. The U.S. requirements may also give rise to issues under other Australian legislation such as privacy and workplace legislation.

The following is a summary of the relevant issues and guidance for ensuring compliance.

7.9.1. U.S. ITAR and FMS controls

The U.S. trade control requirements include the following concepts:

- '**Third country nationals**' who are persons holding the nationality of a country other than the country of the foreign signatory to the relevant Technical Assistance Agreement (TAA), licence or other authorisation.
- '**Dual nationals**' who are individuals who hold the nationality of a foreign country, or have previously held nationality of another country, in addition to the nationality of the any foreign signatories to the TAA, license or other authorisation.

In practice, this means that an individual in Australia who does not hold Australian citizenship (they may be here on a visa or a permanent resident) is considered to be a third country national, while a dual-national is any individual who holds (or has held) citizenship from one or more foreign countries in addition to their Australian citizenship. The U.S. Department of State requires that, in order for any dual or third country nationals to access ITAR or FMS controlled goods, data or services, an authorisation must first be obtained from the U.S. Department of State. Access is generally denied to individuals who are nationals of 'proscribed' countries such as China, North Korea, Syria, Cuba, Iran and other countries listed in ITAR 126.1., unless they hold a current national security clearance.

The issue is further complicated by the fact that for the purposes of ITAR and FMS access, 'nationality' includes consideration of any previous citizenship held, as well as current citizenship. For example, where a person is born in Germany and relinquished their German citizenship when they became an Australian citizen, U.S. law will treat them as being a dual national (a national of both Germany and Australia) because they previously held citizenship of Germany, even though the person is no longer a German citizen.

U.S. trade controls include a number of different exemptions to authorise access by dual and third country nationals, including the following:

- **ITAR §126.18** applies automatically to all access to U.S. ITAR and FMS controlled *unclassified* U.S. defence articles, including technical data, and authorises the employee access providing they are a regular employee of the company and:
    - **§126.18(c)(1) –** hold an Australian security clearance (regardless of other citizenship held), or
    - **§126.18(c)(2) –** satisfy a company screening process for 'substantive contacts' with proscribed countries listed in ITAR 126.1, or

- **§126.18(d) -** are a dual or third country national of NATO countries, European Union countries, Australia, Japan, New Zealand and Switzerland.

- Pursuant to an ITAR **§124.8(a)(5)** request, where §126.18 cannot be applied in the agreement, the Department of State can be requested to vet the subject person, but this may involve assessment in relation to nationality, citizenship or country of birth. Outside of a TAA, this can be requested via a General Correspondence letter to DDTC. Please note para 7.9.2. below.
- Access to *classified* U.S. defence technology is permitted where the individual holds an appropriate Australian security clearance and meets the requirements of the ADOD Security Clause exemption. However, under this exemption there are restrictions on dual/third country national employees who hold, or have held, nationality of a proscribed country. Access is only authorised for these personnel with specific approval of the US Department of State. In addition, this exemption can only be used when the Commonwealth of Australia is a Party to the Agreement or the end-user.
- The **EAR** does not involve considerations of previous citizenship held for licence applications. Only the current country of citizenship and/or country of permanent residency are relevant factors.

It should be noted that the previous §124.16 exemption has been deleted and is now automatically applied under §126.18(d) for all unclassified access. When used in support of a TAA, an NDA is not required from the employee. However, when used in support of other licenses not linked to a TAA, an NDA is required from the individual in support of the application of this exemption.

7.9.2. Australian law – anti-discrimination

Australia does not restrict access to Australian defence technology on the basis of nationality or country of birth.

In addition, Australia has Federal and State laws with respect to anti-discrimination:

- The relevant Federal legislation (*Racial Discrimination Act 1975*) prohibits discrimination on the grounds of 'national origin' and 'race'. The courts have found that neither of these are the same as 'nationality' or citizenship. Nationality or citizenship can change over time whereas national origin is fixed at the time of birth and relates to place of birth or ethnicity.
- Each State and Territory of Australia has legislation which prohibits discrimination on the grounds such as 'nationality', 'national origin', 'race' or 'country of origin'. While the wording of the legislation varies between jurisdictions, the requirements generally prohibit employers discriminating on those grounds when making offers of employment, determining terms and conditions of employment and terminating employment.

7.9.3. Non-Disclosure Agreements

Non-Disclosure Agreements (NDAs) are usually required for each authorised foreign national, including dual/third country nationals that are party to an ITAR agreement (MLA, TAA, WDA) where they do not meet the conditions of exemption 126.18(c)(1) or 126.18(d). The company is required to keep NDAs for five years after termination of the agreement.

7.9.4. Australia's Racial Discrimination Act and the ITAR

Access to ITAR and FMS controlled technology must be carefully monitored by Australian companies, including restricting access to certain files and facilities for some employees that are dual and third country nationals as defined by the ITAR. This requirement has potential to result in discriminatory practices involving the hiring, termination, reassignment and dismissal of staff. Australian companies may need to seek legal advice on their administration of human resources to ensure that in complying with the ITAR they are not in violation of domestic anti-discrimination legislation.

At a federal level, Australia administers the Racial Discrimination Act 1975 (RDA). Section 15 of the RDA prohibits an employer from discriminating against an employee or person seeking employment on the basis of race, colour or national or ethnic origin. Anti-discrimination and equal opportunity legislation at the Australian state and territory level also prohibits discrimination based on national origin. Though the wording of the legislation varies from jurisdiction to jurisdiction, generally employers must not discriminate based on national origin when it comes to making offers of employment, providing advancement opportunities and making decisions to terminate employment. As a practical matter, this means employers must not make decisions based on the employee or job candidate's previous citizenship held. However, the requirements of the ITAR may dictate that the employer do just that to meet the obligations of a licence or ITAR agreement.

Depending on the laws of the particular state or territory, exemptions from compliance with certain provisions of state and territory anti-discrimination legislation may be available to employers for up to 10 years in certain circumstances. Generally, exemption applications are only successful where it can be demonstrated that there is a need to favour a particular group of people over another group as a genuine requirement for the occupation. Legal advice should be sought for your company's particular circumstance.

The use of the previously mentioned exemption §126.18 may provide an appropriate avenue for avoiding such potential discrimination.

7.9.5. Australian Privacy Act and ITAR

In addition to issues raised by Australian anti-discrimination law, the *Privacy Act 1988* (Privacy Act) includes restrictions on when an individual's 'personal information' may be disclosed including to a recipient located outside Australia.

'Personal information' is information or opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and
(b) whether the information or opinion is recorded in a material form or not.

As relevant here, the Privacy Act applies to Commonwealth Government agencies and private sector entities which have an annual turnover of more than $3 million.

ITAR §126.18(c)(2) requires screening records to be made available to the US Government for law enforcement purposes on request. Such records would include personal information.

Employee records exemption

Importantly, the restrictions in the Privacy Act do not apply in relation to 'employee records', that is, information relating to the employment relationship held by the employer. This means that if the information proposed to be made available to the US Government relates to an existing or former employee and is in the context of the employment relationship, the Privacy Act does not apply to that disclosure.

Personal information not in employee record

In the case of personal information relating to other persons such as prospective employees (job applicants), the Privacy Act would apply.

Key considerations under the Privacy Act include:

- Personal information may only be used or disclosed *within Australia* for the primary purpose for which it was collected, with the consent of the individual or if certain requirements apply. Those requirements include where the purpose of the disclosure is directly related to the primary purpose for which the information was collected and the individual would reasonably expect the information to be used or disclosed for that purpose.
- Personal information must not be disclosed *to a recipient outside Australia* unless such steps are taken as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (APPs) in the Privacy Act in relation to the information. The restrictions on disclosing personal information to overseas recipients are set out in APP 8 and are complex. They can include considerations of the relevant privacy or data protection laws in the country of the recipient or require a specifically worded consent from the individual. Under section 16C of the Privacy Act, the entity disclosing the information may be liable for any breach of the Act's requirements by the overseas recipient.

Legal advice should be sought to confirm whether a particular disclosure is lawful under the Privacy Act.

7.9.6. Australian law - industrial legislation

For completeness, it should be noted that actions taken to comply with US trade controls can result in industrial claims being made by the individual such as unfair dismissal claims or adverse action claims under the General Protections in the *Fair Work Act 2009*. Generally, the facts of the particular case need to be assessed to determine the risk of the action being found to be unlawful under Australian industrial law.

7.10. Record Keeping

Maintaining well organised records that are easily accessible and readily available are key to an effective compliance program. A minimum five (5) year retention period applies to ITAR, FMS and EAR (after the project has closed/completed).

One should expect to keep all records relating to licenses and authorisations, transfer and shipment, access, and disposal or destruction of controlled technology.

The EAR is more stringent than the ITAR on record keeping and contains an extensive list of documentation to be retained.

Further details of recordkeeping can be found in the ITAR and EAR Annexes.

7.11. Penalties for Violation of U.S. Export Controls

The scope and nature of penalties for violating U.S. export controls is both significant and vigorously enforced. U.S. authorities apply an extra-territorial approach to any breach of their regime. Penalties can include mandatory process reform, denial of export privileges, debarment, imprisonment for individuals committing criminal offences, and multi-million dollar fines.

In addition to fines and reputational damage, as consequence of violating the EAR or ITAR/FMS Australian companies, including branches of PRIMES, can also be placed on a denial list, preventing US parties from exporting to them.

7.11.1. U.S. Penalties

Violation of U.S. export controls can result in fines and penalties that are even more severe. Below is a chart outlining the fines that may be assigned by the U.S. Bureau of Industry and Security for violation of the EAR and the U.S. Department of State for violation of the ITAR.

These fines[2] and penalties are typically assigned for wilful and/or systematic violations[3].

	Criminal Violations (wilful)	**Civil Violations (undisclosed)**
EAR	Up to $1m USD per violation for entities or $250,000 USD for individuals per violation plus up to 10 years imprisonment of an individual per violation. Both may be levied.	Up to $50,000 USD per violation for both entities and individuals. Imprisonment for up to five (5) years for individuals, or both.
ITAR	Up to $1m USD for entities or individuals per violation and 20 years of imprisonment for individuals for wilful violations, for each violation. Both may be levied.	Up to $500,000 USD per violation for entities or individuals.

While fines can be substantial in value, non-monetary penalties may cost the Australian company more in the form of lost business and reputational damage.

Non-monetary penalties include:

- **Being placed on one of the U.S. "denial lists".** Appearing on a denial list will prevent your company from buying American controlled products or technologies.
- **The Wall Street Journal Effect.** Reputational damage can negatively impact any current or future government contracts.

[2] 22 U.S.C. 2778(c) and (e) for ITAR and Legal Authority Export Administration Regulations as of 21 January 2015 for EAR.

[3] U.S. courts have found that proof of general knowledge of the illegality of the conduct is sufficient to convict a person of a wilful violation of US export laws.

- **Breach of contract.** Existing Defence contracts include clauses on safeguarding controlled technology, and breach of ITAR would result in breach of contractual obligations.
- **Mandatory staffing and external compliance auditing.** Under an ITAR violation, the U.S. State Department may require the Australian company to sign a so-called "Consent Agreement", which would impose demanding and strict requirements to continue accessing ITAR technology, such as increasing compliance resources and various audit and reporting requirements on a periodic basis.

To view a list of companies that have been fined by U.S. State Department, refer:

http://www.pmddtc.state.gov/compliance/poa.html

7.12. Mitigating Penalties

Penalties for violating the ITAR and EAR can be mitigated through voluntarily disclosing the violation to BIS or the DDTC prior to either agency initiating an investigation. Where a disclosure is made, it must be full and complete identifying all violations. Should the BIS or DDTC ask questions following the submission of a voluntary disclosure, and the answers to those questions reveal further violations; penalties for non-disclosure of those violations may be assigned.

A regular publication by the Bureau of Industry (BIS) and Security, U.S. Department of Commerce entitled, *Don't let this happen to you*, which provides recent case histories is available on the BIS website. Consent Agreements, which outline the fines, penalties and required remedial actions that companies convicted of violations are required to take can be found on the DDTC website.

PART 5

Australian Best Practice

8. EXPORT COMPLIANCE AND MANAGEMENT PROGRAM

An Export Compliance and Management Program (ECMP) includes the operational export compliance policies and procedures an organisation implements and a written set of guidelines that captures those policies and procedures. The purpose of an Export Compliance and Management Program (ECMP) is to ensure:

- that the right decisions are consistently being made;
- employees know their export control responsibilities;
- the right policies and procedures are being followed; and,
- the right questions are being asked to ensure that the export compliance and management program is compliant with all relevant regulations and, therefore, consistent with a company's best interests.

Every organisation involved in Import / Export and/or re-transfer / re-export activities needs an ECMP that uniquely addresses their organisation-specific requirements. An organisation's ECMP should be appropriate to the scope of its export / import and re-export / re-transfer activities and to its business circumstances.

There is no generic, off-the-shelf, one-size fits-all ECMP that could completely address all situations of various and different industries and business characteristics. By developing an organisation-specific ECMP that is appropriately tailored to the nature of an organisation's export and re-export activities, an organisation can implement an effective compliance program that works well.

Factors such as the size of an organisation, the end-use and sensitivity of products, the geographic location of business and customers, the relationships with business partners, volume of exports, product restrictions, and complexity of internal export processes will influence how an organisation structures its operational ECMP.

The components of your ECMP should integrate with your normal business compliance approach to standards and regulations. DEC, ITAR, EAR and OFAC regulations compliance is a prerequisite for operating within jurisdictions of DEC, ITAR, EAR, OFAC and other regulations.

The following table identifies possible main components of an ECMP including those proposed by the Bureau of Industry and Security (BIS). These components provide a foundation for the basic structure of your ECMP program, but they do not constitute an exhaustive list; your own list may be longer, reflecting the unique export operations of your organisation.

Main components of an ECMP

Best Practice	Sub-content
Compliance Approach	• Management commitment to a the implementation of a written ECMP • Company Policies • Organisation Structure • Responsibility, Accountability, Consulted, Informed (RACI) • Community of Practice

Agreements and Approvals / Permits	• Australia
	  ○ Export / Import
	  ○ Permits
	• U.S.
	  ○ Re-export / Re-transfer
	  ○ Agreements, Approvals and NDAs
	  ○ EAR
	• Program Management and Sales
	  ○ New Business Checklist
	  ○ Proposal disclaimer
	  ○ Agreements, Licenses and Permits
	  ○ Points of contact

Technology Control Plan	• Tech Data management • ICT plan
Physical Security	• Screening, approval, training and NDA • Customers, third parties, transactions
Human Resources	• Selection, Recruitment, Screening and security clearance
Supply Chain	• Procurement including flow-down of compliance requirement • Supplier and Contractor approval • Receipt and Dispatch • Packaging and identification marking
Training	• Awareness • Training of ECO and all staff
Auditing and Risk Assessment	• Risk Log • Schedule Internal / External Audits
Records	• Refer para 2.8.2 and 3.9
Compliance Issues	• Reporting and Escalating Export Violations. • Corrective and Preventive actions
Internal Communication	• Frequency and method

8.1. Compliance Approach

Companies and other organisations decide what compliance measures are appropriate. As part of their decision analysis, it is recommended that they develop an ECMP that addresses current requirements and has capacity to grow and support future needs.

All compliance programs are different. For example, some companies choose to designate a single employee responsible for the administration, performance, and coordination of export and compliance responsibilities. Other companies decentralise these responsibilities throughout the organisation, but with corporate oversight to ensure essential compliance standards are maintained. The size, organisational structure, and production/distribution network of an organisation are key determinants of where compliance functions and personnel should reside.

Many centralise the administration of training, recordkeeping, dissemination of regulatory material, notification of non-compliance, and audits. However, personnel throughout the company (e.g., in sales and marketing, order entry, or shipping) may perform the actual screening activities against various government lists (of foreign entities that should be avoided, certain end-use and end-user activities, and diversion risk) where first-hand knowledge and information of customers is available.

How you decide to structure your ECMP will depend on your organisation's operations.

One suggestion would be to consider integrating Export Control policies and procedures with an existing Quality Management System (QMS) leading to a common approach to the determination of ownership, responsibility and that Export Control compliance is not a stand-alone activity but rather a specific customer requirement to be addressed and responded to.

8.1.1. ECMP

STEP ONE: GATHER INFORMATION

Before you start writing, gather detailed information and discuss approach with content experts as well as others in your organisation, who hold key information, e.g. long-time staff members, stakeholders, technical staff, and people who will use the procedure. Compile as much information as possible; you want a clear structure and understanding of the detail which can be utilised for specific training events. Reduce the information to generate a document structure that defines your approach to meeting compliance requirements and suitable for helping others understand the importance of your ECMP.

Define the components of your ECMP, procedures and Policies that will assist in determining ownership and responsibility throughout your organisation.

STEP TWO: START WRITING

- Write actions out in the order in which they happen
- Avoid too many words. Just be specific enough to communicate clearly
- Use lists and bullets
- Explain assumptions

- Avoid use of jargon and slang
- Write for your audience, ensure you do not assume a level of knowledge that is not appropriate

STEP 3: MANAGEMENT COMMITMENT

Share the proposed document structure with your management team seeking their endorsement of the ECMP and its further development and implementation.

Highlight the importance of specific assignments within the ECMP and link this to the development of a RACI model.

Identify for each component of your ECMP which position in your organisation has been assigned Responsibility, Accountability, or is to be Consulted or Informed (RACI).

Responsibility for the management of export controls should be fully described, including provision of contact details for managers able to provide guidance and answer export control related questions

The various management roles such as; Export Control Officer, Technology Control Manager, etc, should have position descriptions including reporting and governance arrangements

Descriptions of employee responsibilities and the role and responsibility of contractors and suppliers should be described.

STEP4: COMMUNITY OF PRACTICE

Export compliance is a collaborative, not a competitive, endeavour; reach out to your compliance peers in other companies, even across industry lines, and, of course, also reach out to your partners in the public sector. Discussing and learning best practices, effective approaches, noteworthy experiences, what works and what doesn't, is invaluable in building a strong ECMP to safeguard your company.

Contact: **Centre for Defence Industry Capability** (previously Defence Industry Innovation Centre)

www.business.gov.au/cdic
cdic@business.gov.au
13 28 46

8.1.2. Safeguarding and Monitoring Compliance

Having a rigorous ECMP will help prevent unauthorised access to controlled technologies. A well-implemented and monitored ECMS should include the below nine elements, which will help companies to regulate access and will also serve as a mitigating factor in any enforcement proceeding. The below can be used to evaluate the effectiveness of your ECMP:

- Are management commitment and managerial involvement clearly apparent?
- Are sufficient resources, including qualified and dedicated employees, committed to support the compliance program?

- Are there established mechanisms through which employees feel safe and comfortable reporting concerns regarding noncompliance activity?
- Do you have established compliance policies, procedures, and standards of conduct for export operations and personnel?
- Is there a sufficient level of written operational guidance to ensure day-to-day compliance?
- Are there effective lines of communication throughout export operations?
- Does your organisation provide training to all employees on export-compliance policies and specialised training on policies and procedures for those directly involved in exports and the export-compliance program?
- Have you implemented checks and safeguards, including screening of parties and activities, throughout all export processes?
- Does your program ensure compliance, detect violations through continuous monitoring, and audit systems, and does it ensure appropriate recordkeeping?
- Does your ECMS ensure consistent and quick response to detected violations?
- Does your ECMS have an established procedure for escalating problems and taking corrective action when needed?
- Do you continuously evaluate and modify your program to enhance prevention and detection of noncompliance risks?

Investing in an ECMS that is well integrated into your current business processes can lend predictability, consistency, and security to your export transactions, as you ask the right questions and undertake the right analyses regarding parties to your transactions and uses of your items.

A well-implemented ECMS, including detailed systematic procedures tailored to the specifics of your business, can also lend sustainability and longevity to your business, as well as the business partners you have included in the process, especially given the recent heightened penalties for export violations.

8.1.3. Australian Compliance Program Documentation

DEC has developed the following documents to assist companies in setting up and implementing an internal compliance program (ECMP), as well as additional documents that can assist companies in assessing their export transactions. These documents have evolved from similar material developed by other export control regimes throughout the world and have been modified to make them consistent with Australian export control legislation. Best Practice Guidelines – an outline to the elements of a successful Internal Compliance Program for your company.

- Company Statement of Export Control Principles – an example of a commitment of compliance, written as a statement by the company director, and accessible by all staff.
- Customer Purchase Survey – an example of a compliance questionnaire to be given to a customer on receiving an enquiry or purchase order for your export.

- Export Sales Checklist – an example of a simple risk assessment checklist your company can use to decide if more advice is to be sought from DEC before allowing a sale.

Further information on internal compliance programs is available on the DEC website: http://www.defence.gov.au/ExportControls/InternalCompliance.asp

8.1.4. ECMP elements in a multi-jurisdictional environment - Australia

The organisation may be exposed to multiple export control jurisdictions over the life-cycle of a product or project. For example, components imported for incorporation into products to be on-sold to the world market may invoke both the controls of the country of component origin and controls of Australian government upon export. Complexity can grow significantly as the supply chain and customer base expand, presenting major challenges to the organisation seeking to satisfy the inconsistent conditions of each interested regulator.

Deconstructing the ECMP into major elements is a way of spreading the compliance challenges amongst different parts of the business, and can provide a logical framework for developing instructions and tools that support the implementation of the ECMP objectives. Finding areas of commonalty between the competing jurisdictional interests may simplify the challenge and avoid redundant effort. The organisation's existing toolsets may well be adaptable to supporting the compliance challenge.

8.2. Agreements, Approvals and Permits

8.2.1. Australia

8.2.1.1. Defence Export Permits

Once an item has been determined to be a controlled item, including technology, and the correct jurisdiction has been determined the responsible person in your organisation will apply for a permit to export from DEC.

The responsible person in your organisation shall maintain a detailed register of all Australian Export permits.

Refer DEC License Application Process:
http://www.defence.gov.au/ExportControls/ApplicationProcess.asp

8.2.1.2. Import Permits

- As the Prohibited Imports Regulations are regularly updated, it is prudent to check the DEC website for the most current version and always click the "Latest Version" tab at the top right. Refer:
- https://www.legislation.gov.au/Details/F2016C00795
- A valid import permit must be in place before the controlled goods reach the Australian border. If the permit is not in place:
    - Customs may refuse entry of the goods that are being imported holding them up at the border or even requiring return (re-export needing a DEC permit) to its origin;

- Customs may seize those goods temporarily or permanently; and
- All costs related to import delays, re-exports and seizure will be charged to the company.

Concerning Defence Industry, the most common imports are weapons and explosives. For information that is more specific the Department of Immigration and Border Protection website will provide more information.

www.border.gov.au/Busi/Impo/Proh

8.2.1.3. Brokering

The organisation's marketing and Business Development functions should be cognisant of the regulatory environment, particularly when entering teaming agreements and when sales efforts evolve to the point where transfers of controlled technology can occur.

Consider adapting existing procedures governing the development of prospects and opportunities and the approval of bids to include gates to check for brokering activity.

Your organisation may find that it is acting as a broker and the responsible person in your organisation shall apply for a brokering permit from DEC.

8.2.1.4. Working with DEC

DEC is always willing to help and appreciate any feedback. If you are unsure of anything or need guidance, simply call and ask. If you believe you may have made an error and violated Australian export control laws, it is essential to contact DEC as early as possible.

DEC provides a number of resources to assist you to comply with export control laws:

- face-to-face and online export control training
- tailored outreach to assist individual exporters with specific issues
- the Online DSGL Tool (to help determine if your items or activities require a permit)
- information on the DEC website

http://www.defence.gov.au/ExportControls/Default.asp

You can contact DEC on 1800 661 066 or ExportControls@defence.gov.au .

8.2.2. U.S. ITAR

At one extreme, the formation of Technical Assistance Agreements under U.S. jurisdiction requires specialist knowledge and it is imprudent for the Australian organisation to rely exclusively on the guidance offered by the U.S. applicant. At the other extreme, Export Permits issued by Australia are a comparatively simple proposition for the domestic applicant, not least because proximity to the regulator makes for ease of communication. Australian organisations may also apply directly to foreign regulators for approval to retransfer goods or technology previously acquired, and where the terms of the original licence no longer satisfy the organisation's requirements.

The following are suggested as general principles applicable to all forms of authorisation:

- Obtain and record all authorisations that may be applicable to the organisation's activities. Foreign applicants will not always be in favour of

providing you “their” licences, but where foreign governments assert extra-territorial jurisdictions; your organisation is a risk if it is not fully informed of the licencing conditions.

- Consider extracting relevant particulars of each authorisation, recording these in a central register accessible to down-stream elements of the ECMP, such that those elements are receiving consistent and current information upon which their decisions are based. Down-stream elements that may depend on the central authorisation record include:
  - *Inbound Controls and Tracking* from receipt and whilst artefacts remain within the care and custody of the organisation.
  - The *Access* sub-element, which may need to draw on particular terms of an authorisation.
  - The *Outbound* element, in verifying parties to an authorisation.
  - Plan ahead – get your supply chain fully articulated / ensure all parties are listed (approved) to receive and re-export / re-transfer controlled technology.

8.2.2.1. Re-Export and Re-Transfer

The re-export (or retransfer) of ITAR-controlled Technical Data in Company’s possession is prohibited without prior written U.S. Government approval.

Unless the original export license specifically requested a third party to re-transfer to, then the non-US party must request re-export authorisation otherwise apply exemption 123.9(e) (for incorporated articles) for governments of NATO, Australia, Israel, Japan or New Zealand.

Requesting approval for re-export / re-transfer to a third party shall be managed by the Program Manager through generation of a standard General Correspondence (GC) letter to the (U.S. Directorate of Defence Trade Controls DDTC) including:

- License number or the original export authorisation
- A description of the product, quantity and value
- A description of new end-user (if applicable)
- A description of any change in the information on the original license
- Purchase order from the new buyer

Agreement Types:

- Third Party Re-Transfer Agreement (TPR) under FMS rules
- TAA Technical Assistance Agreement (120.22)
- MLA Manufacturing Licensing Agreement (120.21)
- WDA Warehouse Distribution Agreement (120.23)

8.2.2.2. Sub Licensee Non-Disclosure Agreement

When a third party is not a signatory to an agreement (TAA, MLA or WDA) a sub-license may be utilised for the re-transfer of specific technical data or defence services.

Each sub-licensee shall sign a non-disclosure agreement (NDA) that incorporates the relevant ITAR clauses 124.8 and 124.9 to flow down all necessary clauses via contract, purchase order or other documentation.

Company X Australia could be a third party company under an NDA where the conditions of the higher agreement is passed on to Company X Australia. Similarly should Company X Australia wish to engage a third party an NDA shall be put in place, subject to U.S. government approval, including a flow down of obligations per the higher agreement.

8.2.2.3. Third Party Screening

Best practice screening refer Para 2.3.1.

8.2.2.4. Non-Disclosure Agreements

Non-Disclosure Agreements (NDAs) are usually required for each authorised foreign national, including dual nationals that are party to an ITAR agreement (MLA, TAA, WDA) where they do not meet the conditions of exemption 124.16 or 126.18(c)(1). The U.S. exporter is required to keep NDAs for five (5) years after termination of the agreement.

8.2.2.5. Brokering

The organisation's marketing and Business Development functions should be cognisant of the regulatory environment, particularly when entering teaming agreements and when sales efforts evolve to the point where transfers of controlled technology can occur.

Consider adapting existing procedures governing the development of prospects and opportunities and the approval of bids to include gates to check for brokering activity.

Your organisation may find that it is engaging as a broker, or acting as a broker and the responsible person in your organisation should ensure the organisation is registered as a broker and shall apply for a brokering permit from DEC.

8.2.3. U.S. EAR

Most exports under the jurisdiction of EAR are authorised without an export license (export means out of U.S. to a foreign country) under either a NLR (no license required) or a license exception.

- For Department of Commerce controlled items, apply on-line with Simplified Network Application Process Redesign (SNAP-R). http://www.bis.doc.gov/snap/index.htm

  Refer Department of Commerce License Process.

  - Where an authorisation is not required for the proposed transaction, but the relevant jurisdiction nonetheless imposes restrictions on access to and disposal of the goods or data in question, re-use the tools created to manage authorisations, by creating proxy authorisations with the attributes of the jurisdictions classification. For example, a proposed receipt may be found to be subject to the EAR, but an exemption applicable to Australia may result in no licence being required. The ECCN, its associated EAR conditions and the terms of the exemption might be treated collectively as pseudo authorisation, and recorded as such in the central authorisations register. This approach may also simplify changes to the organisation's controls to accommodate

initiatives of the foreign jurisdictions, such as the U.S. Export Control Reform program, which sees commodities transitioning from the ITAR to the EAR.

8.2.4. Program Management and Sales

Program Management shall maintain a detailed register of all U.S. Agreements and Licences, and if applicable, associated Non-transfer and Use Certificates (DSP - 83).

All TAAs and MLAs, following development, or amendment, by the relevant Program Manager, are to be checked by the head of Programs, ECO and Managing Director and signed in accordance with position authorities.

It may be worthwhile developing a new business checklist to ensure that critical elements of the ECMP are addressed at the beginning of a proposal activity including approval to access technical data for quotation purposes.

Proposals should contain a disclaimer outlining that the receiver of the proposal is responsible for its protection in compliance with ITAR and EAR.

8.3. Technology Control Plan

A Technology Control Plan (TCP) is an essential component of an ECMP. The purpose of a TCP is to describe specific procedures for controlling access to classified and controlled unclassified technical data to prevent unauthorised access. A TCP identifies the activities of an organisation designed to ensure that controlled goods and technology are managed in compliance with legislative requirements, and within the parameters of domestic and foreign jurisdictions that govern exports, re-exports or re-transfers.

Where ITAR controlled technology is being managed by an Australian organisation, a Technology Control Plan should be prepared to outline policies and procedures for managing ITAR controlled technology within the organisation and its third parties, contractors and employees.

The TCP should specify what constitutes controlled technology, outline access control arrangements, and should address the following key areas to help ensure proper management of export controlled material:

- An overarching company policy identifying the relevant regulations and legislation mandating management of controlled technology including technical data.
- Identification of facilities and premises to which the requirements apply
- Identification of company personal to whom the requirements apply
- Controlled technology and other key terminology should be clearly defined
- Linkages to classified materials and systems should be identified, where relevant
- Specific reference/ to both domestic and foreign export control requirements should be well documented
- Guidance on access to IT systems, to prevent unauthorised transfer of controlled technology, should be described and mandated
- Procedures for document control and handling should be adequately described.

Note: A sample TCP is available in Annex E to this guide.

8.3.1. Project / Site TCP

For larger organisations, it may be necessary to produce a specific project or site TCP to manage in detail any controlled technology that cannot be covered in the high level company TCP.

Note: A sample project/site TCP is in Annex E-1 to this guide.

8.3.2. Managing Controlled Technology

8.3.2.1. Suggested practices

- Do not send export controlled files by email or embed export controlled data in email text. Send links to internal pages that require a secure login.
- Do not leave export controlled emails and emails with sensitive attachments in your email folder. Download the information to a secure server and delete the email from your laptop.
- Ensure the transmission of emails that contain export controlled information are stored on a secure server located in Australia and that their transmission is done through secure encrypted services.
- Where possible, Australian companies should consider use of a Virtual Private Network (VPN) to remotely access export controlled information whilst outside of Australia. This removes the requirement to carry export controlled information on the laptop.

8.3.2.2. Australian Controlled Technology

Under Regulation 13E of the Customs (Prohibited Exports) Regulations 1958, a person must obtain a permit from the Defence Export Control Office (DEC) to export controlled goods or technologies in tangible form. For example, controlled technology leaving Australia on a CD, laptop or usb.

If the person supplies that same technology to an end-user overseas in an intangible form (such as by electronic means), the Customs Regulations do not apply. Instead, the Defence Trade Controls Act 2012 (the Act) will regulate this intangible supply.

The measures in the **Defence Trade Controls Act 2012** controls on the supply of DSGL listed technology and services related to DSGL technology and goods. The Act also creates a registration and permit regime for brokering DSGL goods, technology and related services. The Act contains a number of criminal offences to enforce the controls. Australian companies managing export controlled technology need to have a system in place to ensure the technology is safeguarded from unauthorised use and to prevent the violation of export controls.

8.3.2.3. U.S. Controlled Technology

The ITAR controls military technology in both a tangible and intangible form. The EAR also controls certain technologies, including technical data, and has its own definition of 'technology'. In addition, in some instances, the EAR may control the physical item but the technical data associated with the item may remain ITAR controlled. Both the USML and

the CCL must be consulted to determine if the U.S. origin intangible technology you are seeking to export or otherwise transfer is controlled.

Export controls are continually evolving to keep pace with advancements in technology and the way we communicate information; therefore nations are increasingly controlling the intangible transfer of controlled technology, in addition to goods that can be used for a military or WMD programs.

8.3.2.4. General Data Security

It is the responsibility of the Australian company in possession of export controlled technology to safeguard the information. Examples of compliance risks and best practices to address these risks are listed below.

8.3.2.5. Laptop Computers

Leaving Australia with export controlled technology, software or classified data on your laptop may be a violation of Australian or U.S. export controls, unless you have a licence to export the data. This includes attachments and messages in email, especially where emails are downloaded to a laptop through a program such as MS Outlook.

Australian companies should ensure that where laptops with export controlled technology, software or classified data are permitted to leave Australia under licence, that the data is encrypted so that sensitive information can be protected.

8.3.2.6. Electronic Storage of Controlled Information

The proper storage of export controlled data on company servers is an important part of ensuring that controlled data is safeguarded from unauthorised access. Inadvertent access by unauthorised persons may be a violation of Australian or U.S. export controls.

Australian companies should ensure that export controlled data segregated, and where required encrypted so that sensitive information can be protected.

8.3.2.7. Suggested Practices

- On PCs there should be an automated “time-out” process that disables the device until such time as the person using it re-authorises him/herself by way of entering a password;
- On file servers there should be an account/password protection mechanism at the “folder” level of data directory;
- Access to nominated folders to only Authorised persons per a list provided by an employee responsible for export compliance, such as a Technology Control Officer;
- For storage on removable media there should be file encryption mechanism using an encryption method approved by the Company Information Systems Security Officer (ISSO).
- The company’s Technology Control Officer should have nominated “folders” or “directories” on a nominated server for the storage of data relating to controlled technology;

- The Technology Control Officer should regularly provide an up-to-date list of all personnel authorised to access the nominated folders to IT.
- Procedures to destroy/delete export controlled technology at the end of its useful life should be in place.

For further guidance on developing an information security management system, please refer to the ISO 27001 Standard or the Information Security Manual published by the Australian Signals Directorate.

8.3.3. ITAR Controlled Information

All information relating to ITAR-controlled technology that is stored electronically must be protected from unauthorised persons. Australian companies require detailed policies and procedures in place to safeguard ITAR controlled technology. Below is an excerpt from ta typical set of policies and procedures outlining the requirements for accessing, transmitting and transferring ITAR controlled technology.

Measures to secure controlled electronic information, e.g.:

- User ID, password controls, SSL or other approved encryption technology
- Database access may be managed via a Virtual Private Network (VPN).
- Only authorised users can access the site.
- All transmissions of data over the Internet will be encrypted using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology.
- Confidential communications: Discussions about the export-controlled material or projects involving use of the material should be limited to authorised personnel and held only in areas where unauthorised personnel are not present.
- Communications with third parties: Discussions with sub-contractors and other third parties are to be avoided any and only should be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures

8.3.3.1. Electronic Storage of U.S. ITAR-Controlled Technology

All personnel with respect to data relating to ITAR-controlled technology shall adhere to the following rules:

- Such data shall only be placed on removable media for the purpose of transferring such data to another Authorised person;
- All data placed on removable media must be encrypted using the mechanism provided for that purpose;
- Data shall only reside on PCs during the minimum time necessary for working with it;
- Data shall not be saved to, or stored on, any non-removable media within the PC except during the time it is being actively worked on;
- Data stored on servers shall only be placed on nominated servers in the folders nominated for such use.

- Personnel shall not reveal their account names or passwords that pertain to access to data relating to ITAR-controlled technology to any other individual.

8.3.3.2. Transfer or Transmission of ITAR-controlled technology

Transfer involves the transportation of information in electronic form through email or by sending data that has been recorded onto physical media such as portable drives or optical compact disks. Transmission involves the transportation in electronic form by means of electrical or optical signals such as those used on data networks. For the purposes of this document, transfer or transmission only applies to transportation between company facilities or personnel and non-company facilities or personnel.

For either transfer or transmission, the following rules shall apply:

- All information must be encrypted using the mechanism approved by the explicit company policy;
- The sender shall verify, before sending, that the recipient has been authorised, by a person with delegated technology control responsibilities, to access such data. The verification must be obtained in writing and must be retained by the sender as proof that the verification was obtained. Confirmation of authorisation of a recipient can be by way of an e-mail, stating such, from the responsible person;
- The sender shall seek confirmation from the recipient that they have provided a private address to which the sender can send information. Generic addresses used by multiple individuals are not sufficient. The confirmation of address must be obtained in writing and must be retained by the sender as proof that the confirmation was obtained. Confirmation of a private address of a recipient can be that the recipient provided his/her e-mail address to the sender by e-mail.
- The sender shall seek confirmation of delivery of the data to the recipient. Such confirmation must be obtained in writing and must be retained by the sender as proof that the confirmation was obtained.

For transmission, the following applies:

- Confirmation of delivery can be an automated read receipt on an e-mail;
- If confirmation is not obtained within three (3) hours the sender shall contact his/her local party responsible for corporate technology control;
- Encryption and decryption shall be by way of exchange of public keys using transmissions that are separate from that which contains the information being sent;

For transfer, the following applies:

- The transportation shall be by way of registered courier service, approved by U.S. State Department;
- The media shall be enclosed in a double layer of generic wrapping material;
- The nature of the contents shall not be observable from external inspection;
- The sender shall notify the recipient, by means other than the material being sent, of dispatch having occurred;

- The sender shall retain dispatch documentation as proof of transportation;
- If confirmation of delivery is not obtained from the recipient within two business days, or any shorter time considered reasonable in the circumstances, the sender shall notify his/her local party responsible for corporate technology control.

8.3.3.3. Marking ITAR Controlled Information

The ITAR does not provide specific marking requirements, however, it is essential to ensure that items are appropriately identified as ITAR controlled. Hardcopy or electronic documents that contain ITAR controlled Technical Data are often marked with the following statement on the cover page, sleeve, or cover of any design file, software disc, or document (hardcopy or electronic) containing ITAR controlled Technical Data:

8.4. Physical Security

As a minimum, physical security arrangements at all facilities are to include:

- adequate locking devices for external and internal doors, windows, gates and fences;
- security patrols and or monitoring systems to deter and detect unauthorised persons entering the facility; and
- positive identification, recording, and tracking of all employees and visitors.

All facilities may institute additional local procedures/systems that are deemed to be necessary to ensure that physical security is adequate to protect U.S. Controlled Technology or any other Controlled Technologies.

In addition, a Physical security policy should be developed to embrace the following:

- Implementation of a clean desk approach;
    - Document and Data Storage
- Physical and personal security practices to prevent unauthorised access should be described and mandated. Including:
    - Access control
        - Ensure that all access points that have a physical or electronic lock are locked according to controls identified in the policy
        - Perimeter access is monitored
- Visitor identification and control
    - Badging
- Human Resources
    - Recruitment practices
    - Employee responsibilities
    - Termination of employment
- Transport
- Disposal
- Access logs: Physical movement into and out of a designated project area is logged.

- Laboratory compartmentalisation: Project operations are limited to secured laboratory areas physically shielded from access or observation by unauthorised individuals. These areas must remain locked at all times.
- Time blocking: Project operations are restricted to secure time blocks when unauthorised individuals cannot observe or access.
- Locked storage: Tangible items such as equipment, associated operating manuals, and schematic diagrams are stored in rooms with key-controlled access. Soft- and hard-copy data, lab notebooks, reports, and other research materials are stored in locked cabinets.
- Shielding of material: Material is physically shielded from observation by unauthorised individuals by using the material in a secured space, or during secure time blocks when observation by unauthorised persons is prevented.

8.4.1.1. Facility Security

An approved ITAR designated room/s, building or facility (from here on known as facility) is recommended for use for storage of all ITAR controlled physical materials (hardware, software, files, printed documentation).

Any facility that contains ITAR controlled technology should be access controlled and one centralised department in conjunction with the Technology Control Officer (TCO) should manage the access process (room key or card) and all access requests should be made in writing, whereby only approved personnel should be granted access. Regular cleaning, recycling and maintenance services staff should NOT to be provided access to ITAR facilities unless authorised or accompanied/escorted by an authorised person.

ITAR facilities should have a shredder or disposal container for export controlled printed matter.

8.4.1.2. Personnel Security

- Authorised personnel: Personnel who are authorised to use the material must be clearly identified.
- Employee and student responsibilities: Authorised personnel who interface with foreign nationals must receive a copy of the TCP and a briefing that addresses their export control responsibilities.
- Supervisory responsibilities: Supervisors of cleared personnel must ensure that employees and visitors are aware of and knowledgeable about their export controls responsibilities.
- Personnel additions: New authorised personnel must review the TCP and sign TCP certifications
- Personnel changes: Measures for collecting keys to project areas, removing access to project facilities, computers, and other electronic storage devices when personnel leave the project.

8.4.1.3. Access

Drawing on information collected during the Employment and Training phase above, organisations need to consider how they permit members to have access to controlled technologies. The problem becomes more complex if there is significant involvement of US jurisdictions, where account of an individual's nationality (however defined) needs to be taken. One method is the implementation of Approved Team Lists (ATLs). ATLs can be most effective and efficient when:

- Managed close to the team involved (e.g. within a project), where the need for access is best appreciated.
- Are supported by access to centrally stored employee records.
- Are supported by access to stored authorisation details (refer *Licensing* element), whether or not the organisation elects to hold these details centrally.

> **WARNING** - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401 et seq.). Violations of these export laws are subject to severe criminal penalties.

Approval of employee access (depending on applicable jurisdictions) may be dependent upon comparison of employee details with the relevant Control Parameters (established from either a relevant authorisation or the jurisdictions classification of the controlled technology). Jurisdiction and authorisations will also determine the exemptions applicable to dual and third country nationals (where nationality is a Control Parameter).

Efficiencies can be gained when the design of ATLs is considered in concert with:

- the adaptions made to systems used for storing controlled data and tracking controlled hardware;
- Systems employed for the collection of employee data; and
- Systems employed for recording details of authorisations and licences.

Implementation of Access Controls is task distributed between those within the organisation responsible for physical security, information technology administration and security, project team leads, Human Resource team and export control specialists – the latter is likely to be the lead in design and implementation. Where the organisation is presented with complex access scenarios (as in the case where there is a significant U.S. jurisdictional component) investment is planning and cross-functional coordination is likely to yield benefits.

8.5. Human Resources

The U.S. interprets "third country nationals" to include "dual-nationals" – or in Australian parlance, dual-citizens – and any transmission of U.S. Controlled Technology to a dual-citizen is deemed by the U.S. Government to be an export to all countries to which the dual-citizen may have allegiance. This is known as a "deemed export". Access to U.S.

Controlled Technology by dual-citizens must be approved under the relevant U.S. Agreement, or by the prior approval of the U.S. Department of State.

8.5.1. Options for addressing U.S. and Australian requirements

In practice, Australian anti-discrimination law (particularly State and Territory law) means employers must not make decisions based on an employee or prospective employee's nationality, citizenship or country of birth. This may give rise to a potential conflict with some U.S. requirements, such as ITAR 124.8(5) and EAR.

In order to address this, some options include:

- Applying ITAR 126.18 where possible as it can be applied without considerations that would be unlawful under anti-discrimination law. This can be based on either:
    - the holding of a security clearance, or
    - applying an appropriate screening process to identify anyone with substantive contacts to proscribed countries. The Australian Government Department of Defence website provides guidance on implementing screening processes.
- Seeking an exemption under Australian law from anti-discrimination legislation. State and Territory laws generally provide for exemptions to be granted by the relevant anti-discrimination tribunal to permit what would otherwise be unlawful. Generally, exemption applications are only successful where it can be demonstrated that it is a genuine occupational requirement of the position. Legal advice should be sought if it is considered that an exemption may be required to meet the ITAR requirements. There is no process for obtaining an exemption under the Federal anti-discrimination legislation. However, as indicated above, the Federal legislation is less likely to raise issues in relation to compliance with US trade controls.
- While the application of the requirements of EAR involve considerations of the nationality and citizenship, the broad scope of those provisions may mean there is a lower risk of persons being excluded because of those provisions and the risk of there being a contravention of Australian laws.

8.6. Supply Chain

Consideration should be given to making sure all elements of the supply chain have been addressed to mitigate any chance of an unauthorised transfer. The application of the Defence Security and Vetting Service's transport planning guidance for classified material (http://www.defence.gov.au/DSVS/resources/DSM/PUBLIC%20DSM%20Part%202.33%20-%20Annex%20F.pdf) or the alignment to the ISO 28000 Supply Chain Security Standard are useful templates for developing a company's transport policy and procedures. There are also useful supplementary certification and accreditation standards for the ISO 28000 series based on the ISO9000 Quality Management Standards. Consideration can also be given to the **Customs-Trade Partnership Against Terrorism** (C-TPAT) which is a voluntary supply chain security program led by U.S. Customs and Border Protection (CBP) and focused on improving the security of private companies' supply chains with respect to terrorism. As of December 1, 2014, the program has 10,854 members.

Companies who achieve C-TPAT certification must have a documented process for determining and alleviating risk throughout their international supply chain. This allows companies to be considered low risk, resulting in expedited processing of their cargo, including fewer Customs examinations.

8.6.1. Inbound Controls and Tracking

Controlled material (hardware and data) on receipt should be identified, associated with the applicable jurisdiction, export control classification and any relevant authorisations (licences, permits or agreements) – generally, the item's Control Parameters. To avoid delays in receiving goods and data, it is highly desirable that an item's Control Parameters be established in advance of receipt:

8.6.1.1. Procurement

- The organisation's Procurement function can establish Control Parameters at the time of soliciting quotations from potential suppliers. Establishing Control Parameters at this time can also inform source selection (the organisation can consider the risks associated with the export control jurisdictions of various potential suppliers, and include the risk assessment when evaluating competing quotations and proposals).
- Where information obtained by the Procurement function indicates that licencing will be required for the selected item, time and risk associated obtaining these licences can be incorporated in the order or supply contract, and the risks allocated to the appropriate parties.
- By establishing Control Parameters early, opportunity is afforded the Procurement function to liaise with the organisation's Export Control specialists, particularly if the authorisations required a complex, as in the case where a Technical Assistance Agreement might be required in advance of supply.
- The Procurement function would include members trained in the basics of overseas Export Control laws and regulations, to the extent necessary to engage in a meaningful dialog with potential suppliers.
- Establish business rules for obtaining Control Parameters – these might be incorporated in existing Procurement procedures forming part of the organisation's Quality Management System. Forms for soliciting Control Parameters from potential suppliers might be developed. Do not assume that materials supplied by domestic distributors are not controlled by overseas jurisdictions.
- Consider adapting existing purchasing systems to collect and store Control Parameters, making this information available to the organisation down-stream in the supply/production process (e.g. to the inventory management function).
- Consider how to include methods of acquisition not necessarily associated with the Procurement function and purchasing system – e.g. controlled materials supplied free-in-aid by a customer.
- In summary, establish Control Parameters before placing an order or demand for the supply of materials or data.

8.6.1.2. Warehouse and Inventory Management

- With the Procurement function having established Control Parameters in advance of receipt, the task of receiving controlled materials can be simplified at this point. Inbound goods can be matched to Control Parameters by reference to the purchasing system. Where the organisation operates integrated supply and inventory systems, consider adapting this system to allow Control Parameters recorded by the Procurement function to be readily associated with items received into inventory.
- An existing inventory management system may be capable of adaption to allow "tracking" of controlled materials. Tracking requires that the controlled material be identified within the system, and its current location (whilst in the custody and control of the organisation) be recorded and readily available to interrogation.
- Staff receiving controlled goods should have documented processes for:
    - Examining inward goods (particularly the associated receipt documentation) for indications of controlled material <u>not</u> captured in advance by Procurement.
    - Quarantining controlled items until any anomalous records can be resolved by Procurement or the part of the organisation responsible for initiating the supply.
    - Transferring verified controlled materials to the inventory management system and associating the Control Parameters with the item now in stock.
    - Verifying the authority of employees and others to draw controlled material from stock (refer section on *Employment, Access and Training*).
    - Holding controlled stock in secure locations with access restricted to approved persons.

8.6.1.3. Document Management

- Process analogous to the above section on Warehouse and Inventory Management may be required in order to ensure control over received data, and also internally generated data that may be subject to Australian controls.
- Engineering functions are typically the primary users of controlled data and document management systems may well exist within the organisation along with the designated role of document controller or similar. Consider adaption of document management systems to the task of associating stored data with the relevant Control Parameters.
- For data, Control Parameters are more likely to be known from established arrangements with customers and suppliers. For U.S. supply chain partners, Technical Assistance Agreements may also exist. Data transfers
- Consider establishing points of contact within the organisation for the receipt of inbound data. Upon receipt:
    - Data should be held in a staging area with access restricted to a limited number of employees (e.g. documents controllers), pending triage.

- Document Controller will need to identify incoming data. Identification protocols can be established with supply chain partners at the outset of the project. The organisation may require external partners to deliver data only to specified locations, nominated individuals and be accompanied by a transmittal note or similar setting out the Control Parameters.
- Document Controller will transfer verified controlled data to the document management system associating each document with the relevant Control Parameters.
- For documents stored electronically, Document Controller will need to establish permission groups attached to the document or path to the document.
- Documents should have applied (if not already present) a Dissemination Limiting Marker (DLM) that gives a clear warning to any otherwise uninformed reader that the document is controlled and should not be further disseminated without reference to the Document Controller and the ATL.

- The above "receiving" controls should also apply, to the extent practicable, to data generated internally to the organisation:
  - The author can be regarded as the "supplier" for this purpose. Engineering teams will need to establish protocols for identifying:
    - Australian controlled technology they may have created without reference to overseas technologies; and
    - Aspects of the data generated that incorporate or have been derived from data known to be controlled by other jurisdictions.
- The Document Management processes should consider printing and reproduction activities and embody process for the recall and/or destruction of "one time use only" prints and working copies.
- The internal transfer of data between projects can create a risk of control failure. If this is a concern to the organisation, a general approach to this effect internal transfers by following established principles for despatch (see Outbound Controls) and receipt, per above.

8.6.2. Outbound Controls

Outbound controls can be more effectively and efficiently implemented when building on the work done around other elements of the ECMP, particularly the *Inbound Controls and Tracking* and the *Licencing* elements. The immediate challenge of identify and classifying artefacts subject to outbound controls is met down-stream.

Outbound controls may then focus on the following:

- Checking, by reference to the relevant Control Parameters, that the consignee is authorised to receive the artefact. The applicable jurisdiction may require the consignee to be identified in an authorisation, or the consignee's location may need to be within an approved destination. Note the potential for involvement of multiple

jurisdictions. Also note certain jurisdictions (the ITAR) also require the freight forwarder (not a common carrier) to be authorised as an intermediate consignee.

- Checking that shipping documents are correct and include required and desirable information relevant to the consignment's control status:
    - Certain jurisdictions (ITAR and EAR particularly) require the express incorporation of a Destination Control Statement (DCS) on documents associated with the outbound artefacts. Irrespective of any express requirement, good practice is to inform the consignee of the controlled nature of the consignment (as you would have a supplier inform you). To the extent practicable, consider adapting existing systems such that packing lists and transmittal notes (for data) recite Control Parameters already captured in the organisation's inventory or document management system.
    - DCS, where required, should appear on shipping documents and Commercial Invoices, tailored to the requirements of the applicable jurisdiction. The ITAR requires the authorisation, ultimate destination and end-user to be cited. The EAR requires the classification to be cited in certain circumstances. It may be simpler to implement systems that routinely cite the authorisation and classification numbers on all despatch instruments, irrespective of whether or not the destination is domestic or international – an approach which also satisfies the desirability of informing recipients even when a DCS is not mandated.
- Screening of the consignee (and intermediate consignees) may also be verified as part of the *Outbound* element. Referring to the *Third Party Screening* element however, it may be sufficient to verify that the parties are authorised consignees or approved suppliers, as such parties should be subject to screening before entering into contracts and Technical Assistance Agreements.
- The *Outbound* element of the ECMP should include requirements for use of secure packaging (e.g. using tamper evident tape), and requirements to avoid transit of goods through proscribed countries.
- For intangible transfers (i.e. electronic data), shipping documents are replaced by transmittal notes, but otherwise the same pre-shipment checks apply (verification that recipient is authorised and inclusion of DCS where these are required and also the Control Parameters where desirable). Additionally, documents should carry the DLM previously affixed (refer *Inbound Controls and Tracking*). Ideally, transfers will be completed via a Secure File Transfer Protocol. Email, especially in plain text, should not be considered secure.

By integrating *Outbound Controls* with systems established to manage *Inbound Controls and Tracking* and the *Licencing* elements of the ECMP, pre-shipment or pre-transfer checks should not generally require specialist knowledge of export controls, except in exceptional circumstance. Warehouse and Distribution staff of the Document Controller releasing data can largely rely on information collected and verified up-stream of the dispatch point. Checks at the despatch point then come down to review of the documentation for missing, anomalous or conflicting data (in addition to checks normally

associated with despatch, including verification that the content of the consignment matches the paper-work).

"Red Flags" should also be considered as part of the Outbound element.

8.6.2.1. Export Documentation

Documents are to be prepared for the delivery of controlled technology, such as export license, packing list, and commercial invoice.

No shipment or transfer of technology will be made until the license has been approved.

The invoice, packing list and air waybill (where required) should incorporate the Destination Control Statement (as per para 7.6) for items subject to the EAR and ITAR:

In addition to any security markings, Program Managers preparing paper documents that incorporate U.S. Controlled Technology information are to integrate the required non-transfer commitments. For example:

> **WARNING**: Contains US Controlled Technology - Delivered under TAA/MLA [insert reference]. Except as authorised under this Agreement, any transfer to third parties must be authorised by the US Department of Defence Trade Controls.

In circumstances where a TAA/MLA reference number is not available (e.g. for legacy Controlled Technology information/data, by Defence, (and Official Information Security markings had not been applied), the following example statement is acceptable:

> **WARNING**: This document has been developed using US Controlled Technology. Transfer to unauthorised parties is prohibited by the US Arms Export Control Act (title 22, U.S.C. SEC. 2751 ET. SEQ.)

The destination control statement will be used on documents for both foreign and domestic shipments. Documents, not limited to, but must.

8.6.2.2. ITAR / EAR Classification

Ideally the controlled technology being shipped should be identified with ITAR – USML category or EAR- ECCN classification listing any respective exemptions or exceptions.

8.7. Training

8.7.1. Training Requirements

The organisation's Human Resource and Recruitment functions can contribute significantly to the implementation of controls in this area:

- All jurisdictions expect that the organisation's workforce dealing with controlled hardware and data especially will be screened for persons who may have previously been implicated in violations of export controls, bribery or corruption or be politically exposed. The recruitment team can be tasked with implementing screening (see *Third Party Screening* element) to the extent this process applies to new recruits.
- All employees being provided access to controlled technologies should receive at least basic awareness training on export controls before such access is provided.

- U.S. jurisdictions (ITAR, EAR and FMS) in particular embody the concept of “deemed re-export”, involving the transfer of controlled materials to nationals of third countries. Those jurisdictions are inconsistent in their interpretation of nationality and the application of various exemptions for dual and third country nationals. In order the manage access to data and hardware subject to nationality sensitive jurisdictions, the organisation may be required to collect information from its employees regarding present and past citizenships, country of birth, and other indicators of affiliation with third countries. Before collecting such information, organisations should consider their privacy protection and anti-discrimination obligations under domestic legislation, and obtain legal advice.

The organisation may choose to apply screening, training and collection of nationality information selectively (only to individuals required to have access to controlled material) or broadly, to its workforce as a whole and at the point of recruitment. For organisations where a significant proportion of the workforce requires access to controlled material, the broader, up-front approach may be more efficient. An additional benefit of universal coverage is mitigation of risk associated with any inadvertent release or exposure of controlled technology to the “unauthorised” component of the workforce. Universal coverage at recruitment also provides flexibility at a later date when the need arises to transfer personnel between projects and departments. Consider, therefore, integrating screening, training and collection of nationality information into the organisation’s general recruitment and induction procedures.

Beyond induction/awareness training, personnel engaged specifically in export control roles may require further training relevant to their discipline. Examples of specialised training that might be considered are:

- Supply Chain and Inventory Management
- Focussing on the identification of controlled technical data
- Human Resources, in dealing with general recruitment and also the augmentation of the permanent workforce through labour hire and staffing agencies.
- Licencing and agreement formation

8.7.2. Elements of an Effective Program for Training Staff

Training is one of the critical elements of an export management and compliance program. Because export control regulations change and products and their end-uses are continually evolving, it is essential to include a training component in the ECMS. Informed employees/staff minimise the likelihood that inadvertent violations of export laws and regulations will occur. Ambiguities can lead to confusion that could contribute to an inadvertent export violation. The entity, therefore, should be dedicated to updating their export control and compliance knowledge base on a regular basis through training. As important as it is to have export compliance policy and procedures, it is equally important that they be communicated effectively to all employees.

All employees who are involved in export-related functions, including top management, contractors, consultants, and even interns, should fully understand export compliance responsibilities. Personnel should be provided with sufficient training in order to ensure they possess a working knowledge of current export control regulations as well as the

specific requirements of the entity's ECMS. By tailoring training to be job-specific, while also providing the big picture regarding the whole process, including some proliferation awareness, your staff will more clearly understand the importance of their export-compliance roles to the entity and the nation. Including training in performance plans and performance appraisals would institutionalise the training program.

Training should cover processes, responsibilities, obligations, and consequences (positive and negative). One should consider emphasising training in areas of non-compliance. Employees should be required to complete training to learn not only about specific export regulations, but also about the particular products that are exported, ways in which such products can be misused, how to identify illegalities, how to detect suspicious and inconsistent behaviour, and what to do in those circumstances. Providing exercises, problems to solve, and "What if…?" scenarios to work through in training might help in this regard.

Through an effective, compulsory, periodic training program for all associated with export transactions an esprit de corps can be built to ensure that your staff become your compliance partners as you make it easy for them to help you. As you invest in your greatest asset, your people, you go a long way in creating the corporate-culture of compliance, so essential in an ECMP. Provide trainees with awards, prizes, and other recognition during and after training.

When developing a training program to support an export compliance program, the following should be considered:

1. Who will be responsible for overseeing export compliance training?
2. Who will be responsible for conducting the export compliance training?
3. Who should be trained and what types of training will be provided?
4. How often will training be provided and/or required?
5. How will training be documented and training records maintained?
6. Are the concerns of all stakeholder units being addressed in the training program?
7. How will training materials be kept relevant and up to date?

8.7.3. Training to be provided

The person(s) delegated responsibility for oversight of the overall export compliance training program should develop a schedule for training all employees of the entity with direct or adjunct export-related functions. The frequency of the training will depend on a number of variables, including the;

- size of the entity
- complexity of the export operations
- amount of personnel turnover
- frequency of changes in a products
- regulations and policies that control them

It is recommended that a timetable be developed for training new employees and for providing continuing education training for existing employees to reinforce export compliance knowledge, communicate changes in the export control regulations, policies and procedures, and to educate on the application of the regulations to new product lines for export.

Formal export control and compliance training should generally be conducted at induction or re-induction (conducted yearly). The frequency and format of refresher training, however, will vary depending on employee's responsibilities and the nature of the export issues involved. Memoranda, newsletters, or e-mail can be effective on-going venues for reminding employees of the export compliance commitment and advising employees of changes to export regulations or the entity's policies and procedures. Once the overall schedule for training has been determined, the person(s) responsible for oversight of the overall export compliance training program should decide on the target groups of employees to receive training and then customise the content of the training for each group. Group training may include the following broad categories, with, perhaps, subgroups that you determine for training that is more specialised.

- Senior Management Training
- Introductory Training for New Employees
- Intermediate Training for Employees with Export-related Jobs and Functions
- Advanced Training for Export Compliance Personnel

8.7.3.1. Senior Management

Training should be provided to senior management to ensure they are aware and invested in their role and responsibilities for the company's export compliance. Training should include company-specific export issues, provide an overview of the company's export management and compliance program, and explain potential liabilities for noncompliance. Costs and benefits should be discussed, as well as strategies for communicating management commitment, allocating the appropriate resources, and enhancing and nurturing a corporate culture of compliance throughout the organisation. Companies with a Board of Directors or a Board of Trustees should conduct the same basic type of top-level briefing for them, too.

8.7.3.2. Introductory Training for All New Employees

For all new employees, companies should consider providing introductory export management and compliance training. As part of this on-board awareness training process for new employees, companies may want to include a security briefing that covers company-specific threat-diversion awareness and defensive security measures. Introductory training can be accomplished in a variety of ways. New employees can attend an internal company export workshop or an external export seminar. They may can also watch a company video on export management and compliance, read the company's Export Management and Compliance Program Manual, and does a shadow assignment with an experienced export management and compliance employee. Introductory awareness training should generally explain (on a broad level):

a. How an export occurs

b. How exports are approved / denied
c. Licence conditions and exception parameters
d. How a violation occurs (including potential releases of technology)
e. The company-specific “red flags” for potential export violations
f. The national security concerns underlying export compliance
g. The company-specific concerns underlying export compliance
h. How the company’s products relate to those underlying concerns
i. Identification of high-risk areas
j. Technical exchanges through telephone, facsimile, e-mail or in person
k. The employee’s specific responsibilities and the importance of each employee in the overall compliance program
l. The consequences for both the company and the individual employee if an export violation occurs
m. The organisational structure of the company’s export-related departments and functions
n. The identities and contact information of responsible export officials who should be contacted if export issues arise
o. Recordkeeping procedures
p. Employee’s reporting obligations and requirements
q. Expectations regarding audits/assessments.

8.7.3.3. Intermediate Training for Employees with Export-Related Roles

Intermediate training for those employees with export-related jobs or those who regularly deal with export issues should be tailored to the specific job functions of the employees but should also include, at a minimum, the following:

a. Overview of the purpose and scope of export controls
b. Applicable export control regulations including a break-down, in layman’s terms, of the connection between the regulations, the license, and the company’s compliance efforts
c. Company-specific written operational procedures for export management and compliance
d. The company’s licences/agreements including license conditions and licence exceptions
e. The company-specific “red flags” for potential export violations
f. The roles and responsibilities of all company export personnel
g. Employees reporting obligations and requirements
h. Expectations regarding audits/assessments

i. The implications of export violations -- administrative, civil, and criminal penalties, personal liability, firing, etc.

j. Compliance checks and safeguards to be conducted prior to entering into contractual relationships

k. Business development security awareness for marketing abroad

l. Requirements for international travel with products or technical data

m. Export document preparation

n. Recordkeeping requirements

8.7.3.4. Advanced Training for Export Compliance Personnel

For those employees who are directly responsible for ensuring the company's export compliance, it is recommended that they be required to attend advanced formal training on at least a yearly basis. This training may be in the form of on-line classes, in-house seminars, or external seminars. By participating in formal compliance training, these employees can remain current on regulatory requirements, industry practices, and compliance issues.

8.7.3.5. Training Documentation and Records Retention

Maintaining records of training helps a company to track and verify which employees have received training. Training records are the hard-copy proof of assurance that the company's expectations have been conveyed and that employees have been advised of their role in supporting the company's compliance efforts. It is recommended that a training record for each training event be maintained and that record include the date and place of training, the instructor(s) name, the subjects covered, and the identification of the employees who attended the training.

Each employee's personnel file should include a record of all export training received. It is recommended that training records be maintained along with other export controls documents for a period of five (5) years.

8.8. Auditing and Risk Assessment

8.8.1. Effective Audit Program

An effective audit program protects the integrity of your ECMS by verifying that operational compliance procedures within all of the entity's export-related divisions and locations reflect the entity's written compliance procedures, and that procedures are consistent with government export regulations.

To identify and resolve inconsistencies between written and operational procedures, draft an audit/assessment module that answers:

- Who should conduct reviews?
- What procedures should reviews follow?
- What should be audited/assessed?
- How often will reviews take place?

8.8.2. Audit Procedure

An effective audit program evaluates whether what should happen, does, and that what should not happen, does not, on a daily basis. Audits determine if the right questions are being asked throughout the process to ensure exports are consistent with Australian and U.S. export controls and, thus, consistent with the best interest of the company. A company's audit program may consist of the following:

a. Use of experienced audit personnel

b. Verification of checks and safeguards employed by individual business units for each of the key elements of an ECMS

c. Internal corporate audits/assessments

d. Use of external auditors/assessors

e. Reporting, corrective action, and follow-up procedures for audits

8.8.3. Internal Corporate Audits

At the corporate-level, companies should schedule internal audits to be conducted at least on an annual basis on the overall export management and compliance program. These audits should focus on the company's overall export compliance process and the export transactions of specific business units. An export compliance audit should include, but is not limited to the following:

- Interviews with export-related personnel and management
- Analysis of export control checks especially screening practices and internal controls for compliance
- Comparison of operational practices to written procedures
- Review of management commitment
- Review of current policies and procedures including all written guidelines
- Review of training and education programs
- Review of the order processing system
- Analysis of the export authorisation process
- Analysis of the implementation of export licenses including adherence to and tracking of license conditions
- Review of internal assessments
- Review of notifications of any non-compliance
- Review of procedures for corrective action and follow-up
- Review of procedures related to visits or employment of foreign nationals
- Review of technology controls and technology transfers, including via e-mails
- Review of procedural checklists for travel abroad, including for hand-carried items like laptop computers

- Review of recordkeeping practices
- Sample review of export-related documents
- Analysis of sample transactions.

8.8.4. External Audits

It is a good business practice to periodically utilise an outside auditor. External audits can provide an unbiased, third-party evaluation, and validation, of a company's overall export management and compliance program and practices.

8.8.5. Reporting, Corrective Action, and Follow-Up Procedures

Companies should include in their export management and compliance programs the appropriate procedures and practices for audit reporting. Audit reports should be provided to the program office or business unit reviewed and to the appropriate management officials. If an audit's findings raise questions concerning export compliance risks, procedures should also be in place for these issues to be raised to management attention. Procedures should define the requirements for implementing audit recommendations, following-up on corrective actions taken, and reporting on audit recommendations.

8.8.6. Pre-audit Checklist

- Identify business units and personnel to be audited
- Send e-mail notification to affected parties
- Develop a tracking log for document requests
- Prepare audit templates such as interview questions, transactional review checklist, audit report format, etc.
- Each business unit should provide their written procedures related to export compliance before the audit
- Personnel at all levels of the organisation, management and staff, should be interviewed to compare written procedures with actual business practices
- Identify gaps and inconsistencies.

8.8.7. Post-audit Checklist

- Write draft audit report
    - Executive Summary [Purpose, Methodology, Key Findings]
    - Findings and Recommendations [Organise in Priority Order]
    - Appendices [Interview List, Document List, Process Charts]
- Conduct post-audit briefing for affected business units to discuss audit findings and recommendations. Provide draft report. This is an opportunity for business units to address inaccuracies in report.
- Obtain commitment from business units for corrective action. Include, with timeframes, in audit report.

- Brief executive management on audit findings and recommendations
- Track corrective actions. Within the year, audit corrective actions

8.9. Records

Records generated by the ECMP will relate to the above key elements or sub-elements ECMP, which may indicate a logical basis for indexing and storage. Records generated by the ECMP that may need to be readily retrievable to support Assurance activities include:

- Procurement – source records used to establish the Control Parameters of delivered supplies.
- Warehousing and Inventory Management – tracking history up to current location or disposal.
- Document Management – source records used to establish the Control Parameters of received data and tracking history to current location or disposal. Also records associated with retrieval and destruction of limited use copies generated.
- Outbound – transmittal notes for data and despatch documents for hardware with evidence that consignee authorisation was verified before despatch and evidence that Destination Control Statements (where required) have been correctly applied.
- Employment and Training – records, ideally held centrally by Human Resources, of export control training history and any nationality data collected.
- Access – the Approved Team Lists held by each project or product team.
- Licensing – licences, agreements and other forms of authorisation held in a central register. Also preserve records relating to the formation of these authorisations.
- Third Party Screening – records of screenings conducted, ideally held in a central register maintained by the appointed specialist.
- Assurance – audit schedules and audit reports held by the quality control organisation. Additionally, either quality department of the risk assessor should maintain records of any risk assessments performed that have influenced the development of the audit schedule.
- Investigations and Voluntary Disclosures – investigation reports and disclosure correspondence records held by legal.

8.10. Compliance Issues and Violations

8.10.1. Effective Reporting

An essential part of a company's ECMP are procedures which provide clear guidance to all employees, including contract employees, concerning what actions to take in the event of suspected incidents of any export-related noncompliance.

An effective notification program for reporting suspected incidents of export-related noncompliance includes:

1. Management that is fully committed to conducting business fully compliant with necessary regulations (law) foster a safe environment for employees who raise questions or concerns about compliance
2. Internal and external reporting procedures for suspected violations or non-compliances
3. Corrective and disciplinary actions for non-compliance with company compliance policies and procedures and incidents contrary to Australian and U.S. export law.

8.10.2. Investigations and Voluntary Disclosures

U.S. jurisdictions in particular encourage organisations to investigate and disclose potential violations of export control laws and regulations. The making of a voluntary disclosure can mitigate the consequences of an adverse finding. U.S. jurisdictions may seek to impose hefty financial penalties for violations and organisations also risk debarment. Implementing policy and procedure for investigating and disclosing potential violations, and implementing corrective actions flowing from those investigation, adds value to the organisation proportional to the assessed reduction in risk.

Policy and procedure in this area might be owned by the organisation's legal function. Policy should be clear on:

- the individual employee's obligation to report suspected violations.
- Where responsibility lies for making internal determinations on the conduct of an investigation, including:
    - appointing and empowering an investigator, with clear terms of reference.
    - making determinations on whether or not a breach has occurred.
    - authoring, reviewing and releasing disclosures.

8.10.3. Penalties:

It is important to create organisation policies and procedures to ensure compliance with Australian and U.S. export controls. It is also of paramount importance that employees are educated about the importance of export controls and company policies and procedures to ensure compliance with controls.

It is best practice to regularly audit against existing compliance policies and procedures to ensure compliance issues are addressed and corrected immediately and that violations are disclosed to the authorities in a timely fashion.

8.11. Internal Communications

The company's commitment to compliance may additionally be enhanced through less formal means, such as a monthly company Export Compliance Newsletter, a Compliance Awareness Day/Week. The Newsletter may discuss new products, new regulations, new international threats, and input from staff regarding new compliance topics and improvement ideas.

Use of export compliance posters throughout the organisation and occasional distribution of export-compliance DVDs, perhaps highlighting cases in the news of good/bad practices,

or a brief training segment, might also be good ideas to keep staff aware and enhance your corporate culture of compliance

PART 6

USEFUL RESOURCES

These links are correct at time of publishing, however we cannot guarantee that will be the case when you try them. If they do not work, you may be directed to the new link, but in other cases you may need to Google them.

9. Australian and International Links

9.1. Australian Legislation

https://www.legislation.gov.au/

9.1.1. Customs Act 1901

http://www.austlii.edu.au/au/legis/cth/consol_act/ca1901124/

Customs (Prohibited Exports) Regulations 1958
https://www.legislation.gov.au/Details/F2016C00355

Customs (Prohibited Imports) Regulations 1956
https://www.legislation.gov.au/Details/F2016C00585

Defence Strategic Goods List (DSGL)
http://www.defence.gov.au/deco/DSGL.asp

9.1.2. Defence Trade Controls Act 2012

***https://www.legislation.gov.au/Details/C2012A00153* or via**

http://www.defence.gov.au/DECO/DTC.asp

9.1.3. Weapons of Mass Destruction (Prevention of Proliferation) Act 1995

https://www.legislation.gov.au/Series/C2004A04891

9.1.4. Charter of the Nations Act 1945

https://www.legislation.gov.au/Series/C2004A07356

9.1.5. Autonomous Sanctions Act 2012

https://www.legislation.gov.au/Details/C2011A00038

9.1.6. Strengthened Export Controls Steering Group

https://exportcontrols.govspace.gov.au/

9.1.7. Quick Reference Guide (a useful tool to help you locate items in the DSGL) https://dsgl.defence.gov.au/Pages/Home.aspx

9.2. International Organisations, Regimes and Treaties

9.2.1. United Nations http://www.un.org/en/index.html

9.2.2. United Nations Conventional Arms Register
http://www.un.org/disarmament/

9.2.3. United Nations Security Council Resolution 1540
http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540(2004)

http://www.un.org/en/sc/documents/resolutions/index.shtml

9.2.4. United Nations Security Council Resolution 1673
http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1673(2006)

http://www.un.org/en/sc/documents/resolutions/index.shtml

9.2.5. The Arms Trade Treaty
http://www.un.org/disarmament/ATT/

9.2.6. International Atomic Energy Agency (IAEA)
https://www.iaea.org/

9.2.7. The Treaty on the Non-Proliferation of Nuclear Weapons
https://www.iaea.org/publications/documents/treaties/npt

9.2.8. Wassenaar Arrangement: http://www.wassenaar.org/

9.2.9. Australia Group: http://www.australiagroup.net/en/index.html

9.2.10. Nuclear Suppliers Group: http://www.nuclearsuppliersgroup.org/en/

9.2.11. Missile Technology Control Regime:
http://www.mtcr.info/english/index.html

9.2.12. Zangger Committee: http://www.foi.se/en/Customer--Partners/Projects/zc/zangger/

9.2.13. Chemical Weapons Convention: https://www.opcw.org/

9.2.14. Biological Weapons Convention: http://www.opbw.org/

9.2.15. Arms Control Association: http://www.armscontrol.org/

9.3. Key Australian Government Agencies

- Department of Defence
    - Defence Export Controls (DEC)
      Phone: 1800 66 10 66 (02 6266 7222)
      Email: ExportControls@defence.gov.au
      http://www.defence.gov.au/ExportControls/Default.asp

- U.S. Trade Treaty Team:
  Phone: 1800 66 10 66 (+61 2 6266 7222)
  Email: ustradetreaty@defence.gov.au
  http://www.defence.gov.au/ustradetreaty/
- Defence Capability Acquisition and Sustainment Group

  Email: CASG.Communications@defence.gov.au
  http://www.defence.gov.au/dmo/
  - Australian Military Sales Office
    Phone: Telephone: +61 2 6144 2401
    Email: AMSO@defence.gov.au
    AMSO@defence.gov.au
- Defence Science and Technology Group:

  http://www.dst.defence.gov.au/
  Phone: 1300 DEFENCE (1300 333 3623)
  Email: information@dsto.defence.gov.au

- Department of Foreign Affairs and Trade (DFAT)
  Switchboard: +61 2 6261 1111

  Fax: +61 2 6261 3111

  http://dfat.gov.au/pages/default.aspx

  a. United Nations and Autonomous Sanctions
     Email: sanctions@dfat.gov.au
     http://dfat.gov.au/international-relations/security/sanctions/Pages/sanctions.aspx

  b. Australian Safeguards and Non-proliferation Office
     Phone: +61 2 6261 1920
     Fax: +61 2 66261 1908
     Email: asno@dfat.gov.au
     http://dfat.gov.au/international-relations/security/asno/pages/australian-safeguards-and-non-proliferation-office-asno.aspx

  c. AUSTRADE: http://www.austrade.gov.au/
     Contact: http://www.austrade.gov.au/Contact/contact

- Australian Department of Immigration and Border Protection

  Phone: 131 881
  www.border.gov.au
  http://www.border.gov.au/about/contact

- Department of Industry, Innovation and Science: http://www.innovation.gov.au/
  Phone: 13 28 46

  a. Australia's Chief Scientist: http://www.chiefscientist.gov.au/
     Phone: +61 2 6276 1727
     Fax: +61 2 6213 6558
     Email: chief.scientist@chiefscientist.gov.au

b. The Australian Research Council: http://www.arc.gov.au/
Phone: 02 6287 6600
Fax: 02 6287 6601
Email: info@arc.gov.au

- Attorney General's Department: https://www.ag.gov.au/Pages/default.aspx
Phone: 02 6141 6666
- Australian Bureau of Statistics: http://www.abs.gov.au/
Phone: 1300 135 070
- Department of Infrastructure and Regional Development: http://regional.gov.au/
Phone: 1800 075 001

9.4. United States Government

- Department of Commerce: http://www.commerce.gov/
Phone: +1 (202) 482-2000
    - The Bureau of Industry and Security: http://www.bis.doc.gov/
    Contact: http://www.bis.doc.gov/index.php/about-bis/contact-bis
- Department of State: http://www.state.gov/
Contact us Form: https://register.state.gov/contactus/contactusform
    - The Directorate of Defense Trade Controls
    Phone: (202) 663-1282
    Fax: (202) 261-8199
    Email: DDTCResponseTeam@state.gov
    http://www.pmddtc.state.gov/index.html

9.5. Key U.S. Legislation/Regulations

- Export Administration Regulations
http://www.ecfr.gov/cgi-bin/ECFR?SID=15ed890d194fd29ee925c4337ae5edd1&page=browse

- Commerce Control List
http://www.ecfr.gov/cgi-bin/text-idx?SID=04aecb50aefa6aa17bea0a5b01f14eba&mc=true&node=pt15.2.774&rgn=div5#ap15.2.774_12.
- International Traffic in Arms Regulations
http://www.ecfr.gov/cgi-bin/text-idx?SID=adea9ef7326f97967e8e6224ca68807a&mc=true&tpl=/ecfrbrowse/Title22/22CIsubchapM.tpl

    U.S. Munitions List (USML)
    http://www.ecfr.gov/cgi-bin/text-idx?node=pt22.1.121

- Proposed Rules and Final Rules

    Appendix A : Rules Published by the U.S. State Department

    http://www.pmddtc.state.gov/regulations_laws/proposed_rules.html

Appendix B : Rules Published by the U.S. Commerce Department

http://www.bis.doc.gov/index.php/regulations/federal-register-notices

Appendix C : Consolidated list of Proposed and Final rules on ITA website

http://www.internationaltradeadvisors.com.au/index.php/u-s-export-reform/

9.6. Other Useful U.S. Links

Appendix D : "Subject to the EAR" (Part 734): http://www.ecfr.gov/cgi-bin/text-idx?SID=c15ad1e88fe1dbdd190287b336c843c0&node=15:2.1.3.4.22&rgn=div5

Appendix E : Decision Tree (Supp. 2 to Part 732) http://www.ecfr.gov/cgi-bin/text-idx?SID=730862018eff711c1d3ce93a40f14c92&node=15:2.1.3.4.21.0.1.7.21&rgn=div9

Appendix F : Determining jurisdiction (ITAR or EAR) for a product or technical data/ CCL Order of Review (Supp. 4 to Part 774) http://www.ecfr.gov/cgi-bin/text-idx?SID=c15ad1e88fe1dbdd190287b336c843c0&node=15:2.1.3.4.45.0.1.3.91&rgn=div9

Appendix G : BIS Guidance on re-exports: http://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions

Appendix H : De minimis thresholds for foreign-made items incorporating U.S. Controlled Content (Part 734.4): http://www.ecfr.gov/cgi-bin/text-idx?SID=c15ad1e88fe1dbdd190287b336c843c0&node=15:2.1.3.4.22&rgn=div5#15:2.1.3.4.22.0.1.4

Appendix I : General Prohibition Three (Foreign Produced Direct Product Re-exports (Part 736.2)): http://www.ecfr.gov/cgi-bin/text-idx?SID=e4660079f697d192344e4374190fc2e7&node=15:2.1.3.4.23.0.1.2&rgn=div8

Appendix J : Determining licensing requirements for an item controlled on the CCL (Part 738) http://www.ecfr.gov/cgi-bin/text-idx?SID=730862018eff711c1d3ce93a40f14c92&node=15:2.1.3.4.24.0.1.4&rgn=div8

Appendix K : Determining licensing requirements for foreign national access to EAR controlled items http://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-reexport-guidance1

Appendix L : Commerce Control List (Supp 1. to Part 774) http://www.ecfr.gov/cgi-bin/text-idx?SID=c15ad1e88fe1dbdd190287b336c843c0&node=15:2.1.3.4.45.0.1.3.88&rgn=div9

Appendix M : Commerce Country Chart (Supp. 1 to Part 738) http://www.ecfr.gov/cgi-bin/text-idx?SID=c15ad1e88fe1dbdd190287b336c843c0&node=15:2.1.3.4.24.0.1.5.27&rgn=div9

Appendix N : "Specially Designed" Decision Tool http://www.bis.doc.gov/index.php/specially-designed-tool

Appendix O : CCL Order of review decision tool https://www.bis.doc.gov/index.php/export-control-classification-interactive-tool

Appendix P : STA eligibility decision tool https://www.bis.doc.gov/index.php/statool

Appendix Q : SNAP-R https://snapr.bis.doc.gov/snapr/

Appendix R : Using SNAP-R to make classification advice requests (Part 748.3 of the EAR) http://www.ecfr.gov/cgi-bin/text-idx?SID=c15ad1e88fe1dbdd190287b336c843c0&node=15:2.1.3.4.32.0.1.3&rgn=div8

Appendix S : SNAP-R User Manual: http://www.bis.doc.gov/index.php/licensing/simplified-network-application-process-redesign-snap-r

Appendix T : How to complete a BIS licence application (748P) in SNAP-R (Supp. 1 to Part 748) http://www.ecfr.gov/cgi-bin/text-idx?SID=15ed890d194fd29ee925c4337ae5edd1&node=15:2.1.3.4.32.0.1.16.50&rgn=div9

Appendix U : System for Tracking export licence applications (STELA) https://snapr.bis.doc.gov/stela/

- U.S. Export Control Reform www.export.gov/ECR

  Guidance for implementation of an effective Export Compliance Management Program http://www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance/compliance

- ITAR compliance requirements: http://www.pmddtc.state.gov/compliance/index.html
- U.S. trade sanction programs http://www.treasury.gov/offices/enforcement/ofac/

9.7. Training / Assistance

For assistance with training and/or ITAR issues, Australian companies can contact:

- **Centre for Defence Industry Capability** (previously Defence Industry Innovation Centre)

  www.business.gov.au/cdic
  cdic@business.gov.au
  13 28 46

- **International Trade Advisors** (Eva Galfi)
  119 Willoughby Rd
  Crows Nest NSW 2065

  Mobile: 0421 506 095
  www.internationaltradeadvisors.com.au

For Third/Dual Country National enquiries only.

- **Janice Nand**
  Sparke Helmore Lawyers

  Level 29, MLC Centre,

19 Martin Place, Sydney NSW 2000
T: 02 9373 3517 | F: 02 9373 3599 I M: 0416 103 324
E: Janice.Nand@sparke.com.au | www.sparke.com.au

If you are sub-contracting to a Prime company, you should also be able to seek assistance from that Prime to meet your awareness and training obligations.

Annex A: Abbreviations and Acronyms

AECA	**Arms Export Control Act**: The AECA is the statute that authorises the export control activities of the U.S. Department of State.
AG	**Australia Group**: An arrangement among cooperating nations that have agreed to adopt national export controls on dual-use chemical weapon precursors, biological micro-organisms and related equipment to prevent the proliferation of chemical and biological weapons.
AT	**Anti-Terrorism**: Countries subject to AT controls are those on the State Department's list of countries that support international terrorism.
BIS	**Bureau of Industry and Security**: An agency of the U.S. Department of Commerce established by the Export Administration Act that is responsible for administering and enforcing export controls on "dual-use" items.
CCATS	Commodity Classification Automated Tracking System
CCL	**Commerce Control List**: A list of dual use items subject to Bureau of Industry and Security export licence requirements based on their identity.
CFR	**Code of Federal Regulations**: The CFR is the codification of the general and permanent rules of the Executive departments and agencies of the U.S. Federal Government.
CWC	**Chemical Weapons Convention**: An international agreement among nations that agree they will not develop, produce, stockpile, or use chemical weapons.
DDTC	Directorate of Defence Trade Controls (U.S.)
DEC	Defence Export Controls Branch
DFAT	Department of Foreign Affairs and Trade
DoC	Department of Commerce (U.S.)
DoD	Department of Defence (Australia)
DoS	Department of State (U.S.)
DSGL	Defence and Strategic Goods List
DSP	Department of State Publication (U.S.)
EAA	**Export Administration Act**: The statute that authorises the export control and anti-boycott compliance activities of the Department of Commerce.
EAR	**Export Administration Regulations**: Regulations associated with Department of Commerce trade control legislation.
ECF	**Export Control Forum**
ECCN	**Export Control Classification Number**: Individual categories of items on the Commerce Control List (CCL) are identified by an ECCN.

ECMP	Export Compliance and Management Program
FMS	Foreign Military Sale (U.S.)
ITAR	**International Traffic in Arms Regulations**: Governs the export and import of defence articles and services under State Department export licensing jurisdiction.
MLA	Manufacturing Licence Agreement
NDA	Non-Disclosure Agreement
MTCR	**Missile Technology Control Regime**: The MTCR is a multilateral control regime with guidelines that restrict the export of dual use items that may contribute to the development of missiles or delivery systems.
MTEC	**Missile Technology Export Committee**: A U.S. interagency group chaired by a representative of the Department of State (DOS) that reviews export licence applications involving items controlled for missile technology reasons.
NSG	**Nuclear Suppliers Group**: Nuclear Suppliers Group is an international export control regime that focU.S.es on the non-proliferation of nuclear weapons.
ODTC	**Office of Defence Trade Controls**: The office within the Department of State (DOS) that administers and issues licences for defence services and defence articles.
OFAC	**Office of Foreign Assets Control:** OFAC of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries, terrorism sponsoring organisations and international narcotics traffickers based on U.S. foreign policy and national security goals.
RDA	Racial Discrimination Act (Australia)
SME	Significant Military Equipment
SMEs	Small to Medium Enterprises
SNAP-R	Simplified Network Application Processing System – Redesign
STELA	**System for Tracking Export Licence Applications**: An automated telephone voice response system that provides applicants with the status. of their licence and classification applications.
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
TPR	Third Party Retransfer
USML	**United States Munitions List**: The list of defence articles, technology and services under the export and import jurisdiction of the State Department
VPN	Virtual Private Network

WA	**Wassenaar Arrangement**: The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies is a multilateral regime that contributes to regional and international security by promoting transparency and greater responsibility in international transfers of conventional arms and dual-use goods and technologies.
WDA	Warehouse Distribution Agreement

Annex B Compliance Program Best Practice – a U.S. perspective

Comprehensive operational compliance programs include manuals that articulate the processes to be followed in implementing the company program. Important elements of effective manuals and programs include:

- Organisation Structure
    - Organisational charts
    - Description (and flow charts, if appropriate) of company's defence trade functions
    - Description of any management and control structures for implementing and tracking compliance with U.S. export controls (including names, titles, and principal responsibilities of key officers)
- Corporate Commitment and Policy
    - Directive by senior company management to comply with Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR)
    - Knowledge and understanding of when and how the AECA and ITAR affect the company with ITAR controlled items/technical data
    - Knowledge of corporate internal controls that have been established and implemented to ensure compliance with the AECA and ITAR.
        - Examples of detail:
            - Citation of basic authorities (AECA, ITAR)
- Identification of authorised U.S. Government control body (Directorate of Defense Trade Controls ("DDTC"))
- Corporate policy to comply fully with all applicable U.S. export control laws and regulations
    - Compliance as a matter for top management attention that needs adequate resources.
- Identification, duties, and authority of key persons (senior executives, empowered officials) for day-to-day export/import operations and compliance oversight
    - Corporate Export Administration organisation chart
    - Operating Division Export Administration flow chart
- Identification, Receipt and Tracking of ITAR Controlled Items/Technical Data
    - Methodology used, specifically tailored to corporate structure, organisation, and functions, to identify and account for ITAR controlled items/technical data the company handles (trace processing steps of ITAR controlled transactions from the time the company manufactures/receives the item to the time an item is shipped from the company – or in the case of a defence service, when provided).
    - Examples of questions to be addressed:

        - Are appropriate employees familiar with the AECA and ITAR and related requirements, including handling export approvals with certain provisos and limitations?
        - Are company employees notified of changes in U.S. export control restrictions, and are they provided accurate, reliable interpretation of U.S. export control restrictions?
        - What U.S. origin defence articles are manufactured/received by the firm and from whom? How identified and “tagged”?
        - What U.S. origin technical data related to defence articles are produced/received by the firm and from whom? How identified and tagged”?
        - What items are manufactured by the firm using U.S. origin technical data? How identified and “tagged”?
        - What items or articles are manufactured by the firm that incorporates U.S. origin defence articles (components)? How identified and “tagged”?
        - What kind of recordkeeping system does the company maintain that would allow for control of, and for retrieval of information on, U.S. origin technical data and/or defence articles exported to the company?
- Re-Exports/Re-transfers
    - Procedures utilised to (a) obtain written State Department approval prior to the retransfer to a party not included in a State Department authorisation of an item/technical data transferred or exported originally to the company, and (b) track the re-export or re-transfer (including placing parties on notice that the proposed transfers involve US origin products and labelling such products appropriately).
    - Procedure when an ITAR controlled item/technical data is transferred by the company to a foreign national employed at the company.
    - Procedure when an ITAR controlled item/technical data is transferred by the company to a foreign person within the U.S.
    - Procedure when ITAR controlled technical data or defence articles are transferred from the company to a foreign person outside of the U.S.
    - Procedure when an ITAR controlled item/technical data is to be used or transferred for an end-use not included in the State Department authorisation.
- Restricted/Prohibited Exports and Transfers
    - Procedure for screening customers, carriers, and countries.
    - Screening procedure for high-risk transactions to combat illegal exports/retransfers.
    - Procedures to investigate any evidence of diversion or unauthorised use of U.S. origin products.

- Recordkeeping
    - Description of record systems concerning U.S. origin products.
    - Procedures for maintaining records relating to U.S. origin products for five years from the expiration of the State Department license or other approval.
    - Regular internal review of files to ensure proper practices and procedures by persons reporting to top management.
- Internal Monitoring
    - Perform audits periodically to ensure integrity of compliance program.
    - Emphasis on validation of full export compliance, including adherence to license and other approval conditions.
    - Measurement of effectiveness of day-to-day operations.
    - Adopt procedure for highlighting any compliance areas that needs more attention.
    - Report known or suspected violations to Corporate export administration office.
    - Effective liaison and coordination with Ombudsman.*
    - Examples of detail:
        - Specific description of procedures (examination of organisational structure, reporting relationships, and individuals assigned to export/import controls process.
        - Random document review and tracing of processes.
        - Review of internal recordkeeping, communications, document transfer, maintenance and retention.
        - Conclusion and report of violations to Corporate Export Administrator.
        - Coordination with Ombudsman.
- Training
    - Explanation of company training program on U. S. export control laws and regulations.
    - Process to ensure education, training, and provision of guidance to all employees involved on exports (including those in departments such as Traffic, Marketing, Contracts, Security, Legal, Public Relations, Engineering, Executive Office).
- Violations and Penalties
    - Procedures for notification of potential violations, including use of voluntary disclosure and Ombudsman to report any violation of the company's internal control program or U.S. export controls.

- Emphasis on importance of compliance (to avoid jeopardising corporate business and severe sanctions against the Corporation and responsible individuals).
- Description of AECA/ITAR penalties.
- Written statements and procedures to foster employee discipline (e.g., keying certain types of advancement to compliance understanding and implementation, and establishment of internal disciplinary measures.

Annex C: International Traffic in Arms Regulations (ITAR)

The U.S. Government views the sale, export, and re-transfers of Defence articles and Defence services as an integral part of safeguarding U.S. national security and furthering U.S. foreign policy objectives. Authorisations to transfer Defence articles and provide Defence services, if applied judiciously, can help meet the legitimate needs of friendly countries, deter aggression, foster regional stability, and promote the peaceful resolution of disputes. The U.S., however, is cognisant of the potentially adverse consequences of indiscriminate arms transfers and, therefore, strictly regulates exports and re-exports of defence items and technologies to protect its national interests and those interests in peace and security of the broader international community.

The Arms Export Control Act (AECA) provides the authority to control the export of defence articles and defence services from the U.S. The AECA charges the U.S. President to exercise this authority, which has been delegated to the Secretary of State. The AECA is available through the DDTC Web site.

The International Traffic in Arms Regulations (ITAR) implements the AECA. The ITAR regulates the export, re-export and retransfer of Defence articles, including hardware and technical data, where these articles are listed on the United States Munitions List (USML). The USML is the list of articles deemed strategic to U.S. national security and military capability. It can be found in Section 121.1 of the ITAR. The ITAR and USML are updated and revised to reflect change in the international political and security climate, as well as technological development. Defence articles made outside the U.S. (e.g. Australia) are also subject to the ITAR where the article contains any amount of ITAR controlled hardware, software or technical data. In addition, the ITAR regulates the provision of defence services, including training on, maintenance of, and upgrades to articles subject to the ITAR.

Exemptions

The ITAR provides for several exemptions to the requirement that a licence be obtained in advance of exporting, re-exporting, retransferring or granting access to ITAR controlled technology. These exemptions carry significant conditions and recordkeeping requirements that must be adhered to in order to prevent committing an inadvertent violation.

Records related to the use of exemptions that must be kept include:

- A description of the defence article, including technical data, or defence service;
- the name and address of the end-user and other available contact information (e.g., telephone number and electronic mail address);
- the name of the natural person responsible for the transaction;
- the stated end-use of the defence article or defence service;
- the date of the transaction; and
- the method of transmission.

The person using or acting in reliance upon the exemption shall also comply with any additional recordkeeping (and reporting) requirements enumerated in the text of the regulations concerning such exemption.

Record Keeping

Generally speaking, any documentation or record related to an ITAR controlled project, shipment, agreement, licence or licence exception/exemption must be maintained for five years after the project, shipment, agreement, licence or licence exception/exemption has been finalised. With the ability to request extension of Agreements, it may be that records as old as 20 years will be retained in relation to a project involving ITAR controlled technology. Specific recordkeeping requirements can be found in the following regulations, but not all will apply to Australian companies:

1. CFR 123.22—Filing, Retention and Return of Export Licences and Filing of Export Information
2. CFR 123.26—Recordkeeping Requirements for Exemptions
3. CFR 124.4—Deposit of Signed Agreements with DDTC
4. CFR 124.5—Proposed Agreements that are not Concluded
5. CFR 124.6—Termination of Manufacturing Licence Agreements and Technical Assistance Agreements

It is important to note, especially for those companies utilising the Australia- US Defence Trade Cooperation Treaty that records related to the use of exemption must also be kept for five years from the date of export in accordance with 22 CFR 123.26 and the specific requirements outlined in the exemption.

Non-Transfer and Use Certificate (DSP-83)

A completed Non-transfer and Use Certificate (DSP-83) may also be required for exports of significant military equipment, or classified equipment or data prior to export from the U.S. The DSP 83 provides an assurance that the sensitive goods will be protected from unauthorised access, including re-export, resale or disposal. Allowing access for employees that are prohibited from accessing the equipment or data under a licence, licence exemption or other authorization is tantamount to an export that violates U.S. export controls.

In most cases, the ‘foreign end user’ on a DSP-83 will be the Commonwealth project office or facility. Within Australia, only Defence Export Control is authorised to sign the foreign government certification block on the DSP-83.

The U.S. Department of State requires that this completed form DSP-83 be included as a part of an application for authorisation to export significant military equipment and classified equipment or data. The form DSP-83 must be completed by the appropriate foreign persons (e.g., consignee, end-user, government) and forwarded to the U.S. Department of State through the U.S. person making the application.

Item 1. The U.S. Department of State will enter the application number when the form DSP-83 is submitted with the application. The U.S. applicant must provide the application number when form DSP-83 is submitted separately from the application.

Item 2. Show the name of the U.S. person submitting the application to the U.S. Department of State.

Item 3. Show the foreign person that will receive the articles/data for end-use. A bank, freight forwarding agent, or other intermediary is not acceptable as an end-user.

Item 4. Show the country in which the articles/data ultimately receive end-use.

Item 5. Show precise quantities of the articles/data. List each article/data clearly, giving type, model number, make and (if known) U.S. military designation or national stock number. When components and spare parts are involved, fully identify the minor component, major component and end item in which they will be used (e.g., turbine blades for C-34 jet engine for F24B aircraft). Give a separate value for each major component. Values must represent only the selling price and not include supplementary costs such as packing and freight.

Item 6. To be completed by the foreign person who has entered into the export transaction with the applicant to purchase the articles/data for delivery to the end-user. This item shall be completed only if the foreign consignee is not the same as the foreign end-user.

Item 7. To be completed by the foreign person, in the country of ultimate designation, who will make final use of the articles / data.

Item 8. When requested by the U.S. Department of State, this item is to be completed by an official of the country of ultimate destination having the authority to so commit the government of that country.

Item 9. Certification of U.S. applicant.

Exports under a DSP- 5 licence from the DDTC

Where export of U.S. ITAR controlled equipment and technical data to an Australian party occurs under a DSP-5 licence, there are restrictions on dual or third country national employees accessing the ITAR articles, even when the dual or third country nationals are part of a company's bona fide workforce. Section 126.18 of the ITAR and the FAQ on Dual and Third Country Nationals (available on the U.S. DDTC website) outline these restrictions.

Australian companies receiving ITAR controlled articles under a DSP-5 must ensure that either:

- The dual or third country national employee has a security clearance from the Australian government.

- The dual or third country national employee has undergone a screening procedure to ensure there is no likelihood of an unauthorised re-export or retransfer to a 126.1 country.
- Approval for accessing the ITAR controlled article(s) on the DSP-5 licence is granted to the Australian entity by way of General Correspondence from the DDTC.

Where DSP-5 exports from the U.S. are executed in support of an agreement (TAA/MLA/WDA) then it is recommended that the nationality access provisions of the associated agreement also apply to access to equipment or technical data provided via the DSP-5.

Reporting Violations

Whilst disclosing violations of the ITAR may mitigate fines, penalties and other consequences, it by no means guarantees amnesty from fines and penalties levied by the U.S. State Department. Australian companies considering making voluntary disclosures should therefore be prepared to face enforcement consequences. As the weight given by the US State Department's DDTC for making a voluntary disclosure is solely within the agency's discretion, it is difficult to estimate to what level penalties will be mitigated. However, the risk of not disclosing violations is that they will eventually be discovered (as they have been on numerous occasions in the past) and the ensuing enforcement action will be more aggressive and penalties greater than they would have been had the violation been disclosed in advance of an investigation.

When making a disclosure to the DDTC, or any government agency, it is important to ensure all instances of the violation(s) have been discovered and all information in the disclosure is factually correct. Before making a disclosure to the DDTC, the Australian company must conduct a thorough review of all transactions where a possible violation is suspected. A thorough internal review should be conducted to uncover all relevant facts, prepare the narrative of the violation, and develop corrective actions. The development and implementation of corrective actions that prevent the recurrence of the violations can be an important part of the disclosure. It is required that disclosures to the DDTC be signed by a company official to make the disclosure valid.

Violations/Voluntary Disclosures

Many U.S. Exporters practice the policy of regularly submitting voluntary disclosures to the U.S. Government when they identify a violation of the export regulations. Both the Commerce and State Department's view the practice of submitting disclosures as a mitigating factor in determining penalties. A company that regularly reports violations is demonstrating that it has made a commitment to export compliance and operates a healthy compliance program, which identifies mistakes made by its employees.

Given the complexity of the U.S. export control regime it is unlikely that a company could get by without making a mistake, so companies that do not report their errors,

but make a lot of exports, eventually become the targets of investigation by the regulating agencies.

Voluntary Disclosures can delay or even derail an international program relying on technical interchange or engineering collaboration, as often the company making the disclosure is forced to put the program on hold while they review the circumstances behind the violation and take steps to ensure it does not occur again. In addition, if the nature of the violation was that an export occurred without a licence, then most often the company will halt all exports until the appropriate licence has been obtained. In some cases, it can take as long as 3 months to get a licence approved.

The State Department strongly encourages the disclosure of information to the Directorate of Defense Trade Controls by persons that believe they may have violated any export control provision of the Arms Export Control Act, or any regulation, order, license, or other authorisation issued under the authority of the Arms Export Control Act. The Department may consider a voluntary disclosure as a mitigating factor in determining the administrative penalties, if any that should be imposed. Failure to report a violation may result in circumstances detrimental to U.S. national security and foreign policy interests, and will be an adverse factor in determining the appropriate disposition of such violations.

Annex D: Export Administration Regulations (EAR)

The EAR is administered by the United States Department of Commerce, **Bureau of Industry & Security (BIS)**. The Export Administration Regulations (EAR) governs the export, re-export and retransfer of military and commercial items subject to its jurisdiction. Most of the controlled items are enumerated on the EAR Commerce Control List (CCL). The CCL can be found in Supplement 1 to part 774 of the EAR. U.S. origin military and dual use technology not controlled by the ITAR is subject to the EAR, even if not listed on the CCL. Military and commercial items made outside the U.S. (e.g. Australia) may also be subject to the EAR depending on the amount of U.S. controlled content these items contain. Generally, the *de minimis* threshold is 25% U.S. controlled content. If the foreign made item contains less than 25% U.S. controlled content, it will not be subject to the EAR. However, there are exceptions to this general threshold. For example, there is also a lower (10%) threshold for items destined to a U.S. arms embargoed country. Furthermore, some sensitive items on the CCL, for example those with Export Control Classification Numbers (ECCN) in the "600 series" or those listed in Part 734.4(a)(3) have no de minimis threshold.

In addition, the EAR implement anti-boycott law provisions requiring regulations to prohibit specified conduct by United States persons that has the effect of furthering or supporting boycotts fostered or imposed by a country against a country friendly to United States, such as Israel.

The export control provisions of the EAR are intended to serve the national security, foreign policy, non-proliferation, and short supply interests of the United States and, in some cases, to carry out its international obligations. Some controls are designed to restrict access to dual use items by countries or persons that might apply such items to uses inimical to U.S. interests.

There can be no substitute for consulting the most current U.S. legislation where questions about U.S. export controls arise. The EAR and the CCL can be found on the BIS website under the Regulations tab.

Working with the EAR

The EAR contains many sections that must be consulted in order to determine whether a licence from the BIS will be required prior to export.

The ability for Australian companies to make a direct licence application with BIS makes it easier for Australian companies to obtain a licence for the export of EAR controlled items, however, understanding the complexities of the EAR can be quite challenging,

Australian companies must consult several different sections of the EAR to determine:

Is the item subject to the EAR? (If Australian made, does it meet U.S. de minimis thresholds?) The end of this document contains several links under the heading **Determining if an item is subject to the EAR**, which may assist.

- The classification of the item on the Commerce Control List (CCL)

- Whether General Prohibitions apply
- The reasons for control
- Whether or not the reason for control triggers a licence requirement
- Where a licence is required, is a licence exception is available?

The ability to comply with the EAR necessitates that the employee reading the regulations is able to:

- Read and interpret US legal and regulatory language
- Become a self-taught expert on the classification and controls related to the technologies with which the company works
- Communicate the regulatory requirements to other company stakeholders to ensure technology subject to the EAR is identified, licences are obtained where required, and proper documentation is retained for both items exported under licence and items exported under a licence exception.

EAR Classification

The EAR CCL is a list of ECCN describing the items controlled, the destinations to which they are controlled, licensing requirements and available licence exceptions.

The Commerce Control List has 10 Categories, numbered 0 through 9, and five Product Groups, designated by the letters A through E.

The ECCN begins with the category number, followed by the product group letter. Next, the types of control are listed. For example, where the number 6 is the third character, this indicates that the item is a “600 series” or former USML item. An item may be, and often is, controlled for more than one reason. The combination of category number, product group, and reasons for control make up each ECCN. ECCN are always 5 characters.

Commerce Control List Categories	
0	Nuclear & Miscellaneous
1	Materials, Chemicals, Microorganisms and Toxins
2	Materials Processing
3	Electronics
4	Computers
5 Part 1	Telecommunications
5 Part 2	Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

Types of controls (2nd and 3rd digit following letter)

0 - National Security (Wassenaar)

1 - Missile Technology Control Regime

2 - Nuclear non-proliferation reasons

Five Product Groups	
A	Systems, Equipment and Components
B	Test, Inspection and Production Equipment
C	Material
D	Software
E	Technology

Controls and Best Practices

When classifying an item that is likely subject to the EAR the following steps should be followed. Please note that the Commerce Control List Order of Review, which can be found in Supplement 4 to Part 774 of the EAR, is the official guidance on EAR classification.

a. EAR Classification Procedure

- Review the U.S. Munitions List to ensure the item does not fall/remain under the jurisdiction of the ITAR.
- Determine if the item is subject to the EAR as per origin or de minimis requirements. Where the item is subject to the EAR, review the Commerce Control List (CCL).
- Review the ten Category headings in the CCL first. Categories should be compared to determine all possible categories of the CCL that may cover the item.
- Once applicable categories are determined, identify the appropriate product group (A-E).
- Read the ECCN in the selected product group. Begin with the 600 series ECCN as they 'trump' other ECCN. Look for enumerated controls. Review (.a-.w) first, and then (.y). If the item is enumerated, that is the ECCN.

Note: If the item is not enumerated in the 600 series ECCN, then determine if the item is "specially designed" (under the EAR definition of the term) for a 600 Series item or USML article. If yes, the item will be classified in the (.x) paragraph of the 600 Series ECCN. "Specially Designed" Decision Tool http://www.bis.doc.gov/index.php/specially-designed-tool

- If the item does not meet the definition of "specially designed", then consider ECCN other than the 600 series ECCN.
- Where a person is unable to choose between two or more ECCN in making a classification determination, they may make an application for a classification advice to BIS using SNAP-R.
- Once the ECCN has been determined, document the ECCN and the logic and information used to determine that ECCN in the classification matrix. Any documentation used to determine that the item meets the definition of "specially designed", or to determine that it does not meet a particular part of the definition, should be noted. Any advice from an engineer or third party that was used to determine the ECCN should also be documented. Note the name and contact details of engineers and suppliers consulted in obtaining information about the product should. Any de minimis calculation methods should also be recorded. Where licence exceptions are available for the export/re-export/retransfer of the item, the exception and its conditions for use should be recorded.

- Where there is no applicable ECCN for the item on the CCL, but the item is subject to the EAR, the item's classification will be EAR99. EAR99 items may require a licence to some destinations, end users or end uses.

b. Classification of an Item and/or Interpretation of the EAR

In the event that the classifier is unable to classify an item, he/she may submit a classification request to BIS in SNAP-R and ask for guidance. Classification requests may in some cases also be used to ask for assistance in determining whether a particular item meets the EAR definition of "Specially Designed" in Section 772.1.

In some cases, grey areas may exist in the interpretation of the EAR as it relates to a particular export or activity. In this instance, an Advisory Opinion can be requested from BIS to provide clarity as to how BIS interprets the EAR in relation to the export or activity in question. Advisory opinions are commonly used to ask BIS to determine whether a licence is required for a proposed export or activity. Section 748.3 of the EAR provides guidance on requesting classification requests and advisory opinions.

Advisory Opinions and responses to Classification Requests from BIS are not binding. They may not be relied upon as evidence of the U.S. Government's opinion that an item is either subject to the EAR or not subject to export control jurisdiction of another agency of the U.S. government. The Australian exporter remains responsible for determining the jurisdiction of the article/item, the correct classification of items and for correctly interpreting the EAR. However, guidance provided by BIS should be kept on file as support for the final determination of the ECCN or interpretation of the EAR made by the Australian company.

Licensing

The EAR controls items subject to the EAR in a different way to how the ITAR controls items on the USML. 'Commerce Department Licences' for re-exports and retransfers of items subject to the EAR are not required in every instance. The licensing requirements for a particular item will depend on both the item's classification and the destination to which is it being re-exported or retransferred. The eligibility to re-export or retransfer an item without a licence, or under a licence exception, is determined by a company's self-assessment of the transaction.

BIS licences may contain conditions related to their scope including the authorisation of particular activities, quantities, values, and authorised parties to the transaction. BIS licences typically have more conditions than State department approvals. Companies are responsible for communicating the conditions of BIS licences to the appropriate parties at their business unit. It is a violation of the EAR to fail to adhere to the conditions of a BIS licence.

BIS licences are valid for four (4) years. It is possible to request that changes be made to BIS licences once issued. Section 750.7(c) of the EAR describes the process for requesting non-material changes to a licence and the types of changes that are permissible. Where the required change is not listed in this section of the

EAR, a “replacement licence” will need to be obtained from BIS to accommodate the licence amendment request.

Licensing requirements depend on two key factors. The first is the list of restrictions on the items themselves, which appear in the *Licence Requirements* section of the ECCN. The second is the destination of the item’s export. The restrictions listed in the ECCN and the destination of the export (an export includes any re-export/retransfer or deemed export) need to be understood to determine the licensing requirements for a particular transaction. EAR99 items may also have licensing requirements for to certain destinations, end-uses and end-users. Refer to the ten General Prohibitions listed in Part 736 of the EAR.

Reading the Commerce Country Chart

The Commerce Country Chart, found in Supplement 1 to Part 738, needs to be read in conjunction with the reason(s) for control listed in the ECCN to determine if a licence is required for an export of an item to a particular country. This includes determining if a licence is required for foreign nationals of certain countries to access the item, which is known as a “deemed export”.

First, ensure the item is subject to the EAR and that the classification of the item is correct to the sub-paragraph level. Note the reasons for control listed in the Licensing Requirements section of the ECCN.

On the left hand side of the country chart, look for the row where the country to which the export is going appears.

All of the reasons for control are listed across the top of the chart in the headers. Identify each column containing a reason for control that applies to your ECCN. Most ECCN have more than one reason for control listed in the ECCN.

Identify the cells where the control header and country intersect. If there is an ‘x’ in any of the cells, the export will need a licence, unless you can find an applicable licence exception. Determine if there is an ‘x’ in the cell for each of the reasons for control. If there is no ‘x’ in any of the cells, then the export does not require a licence from BIS.

for **example**,

You are re-exporting ECCN 7A006 (airborne altimeters) to Germany. The reasons for control listed in this ECCN are:

Reasons for Control: NS, MT, AT

Control(s)	Country Chart
NS applies to entire entry	NS Column 1
MT applies to entire entry	MT Column 1
AT applies to entire entry	AT Column 1

To determine whether or not a licence is required for the re-export of an item classified ECCN 7A006 to Germany, one must look at the country chart and identify where there is an ‘x’ in any cell where the row for Germany and the columns containing the controls (NS, MT, AT Column 1) intersect.

Commerce Country Chart

Reason for Control

Countries	Chemical & Biological Weapons			Nuclear Nonproliferation		National Security		Missile Tech	Regional Stability		Firearms Convention	Crime Control			Anti-Terrorism	
	CB 1	CB 2	CB 3	NP 1	NP 2	NS 1	NS 2	MT 1	RS 1	RS 2	FC 1	CC 1	CC 2	CC 3	AT 1	AT 2
Georgia	X	X	X	X		X	X	X	X	X		X	X			
Germany[2]	X					X		X	X							
Ghana	X	X		X		X	X	X	X	X		X		X		
Greece[3]	X					X		X	X							
Grenada	X	X		X		X	X	X	X	X	X	X		X		
Guatemala	X	X		X		X	X	X	X	X	X	X		X		
Guinea	X	X		X		X	X	X	X	X		X		X		
Guinea-Bissau	X	X		X		X	X	X	X	X		X		X		
Guyana	X	X		X		X	X	X	X	X	X	X		X		
Haiti	X	X		X		X	X	X	X	X	X	X		X		
Honduras	X	X		X		X	X	X	X	X	X	X		X		
Hong Kong	X	X		X		X		X	X	X		X		X		
Hungary[3]	X					X		X	X							

As illustrated above, Germany has an ‘x’ in both the NS1 and MT1 columns. For this reason, a licence from BIS will be required unless the re-export/retransfer is eligible for a licence exception.

Because the licensing requirements for an item vary based on the destination, it is important to perform this analysis for each export transaction where an item subject to the EAR is involved. One cannot simply record whether or not a particular item has a licence requirement or is eligible to use a particular licence exception. Each separate transaction must be examined. Furthermore, the ECCN list of items must also be carefully reviewed for each transaction, as licensing requirements can be different at the sub-paragraph level.

For example, 9A610 (Military Aircraft and Related Commodities) specifically excludes certain items classified in subparagraph “.y” from specific controls, as illustrated in the Reasons for Control table (below).

9A610 Military Aircraft and Related Commodities

Reasons for control: NS, RS, MT, AT, UN

Control(s)	Country Chart
NS applies to entire entry except 9A610.u, v, w, and y.	NS Column 1
RS applies to entire entry except 9A610.y	RS Column 1
MT applies to 9A610.u, v and .w	MT Column 1
AT applies to entire entry	AT Column 1
UN applies to entire entry except 9A610.y	See 746.1(b) for UN controls

License exceptions

LVS: $1500

GBS: N/A

CIV: N/A

STA: (1) Paragraph (c)(1) of license exception STA (740.20(c)(1) of the EAR) may not be used for any item in 9A610.a (i.e., “end item” military aircraft), unless determined by BIS to be eligible for license exception STA in accordance with 740.20(g) (License exception STA eligibility requests for “600 Series” end items). (2) Paragraph (c)(2) of License exception STA (740.20(c)(2) of the EAR may not be used for any item in 9A610.

Australian Guide to Export Controls and Best Practices

Licence Exceptions

Licence exceptions allow an exporter to export, re-export and retransfer the item without having to obtain a licence from BIS. Approval from BIS is not required to use licence exceptions in most circumstances. For many items in the EAR, licence exceptions are available for export to certain destinations. There are two types of licence exceptions, item based and transaction based. Item based licence exceptions are noted in the ECCN of each item, as illustrated in Figure 2 above.

Part 740 of the EAR contains information about licence exceptions that are non-ECCN driven but are instead transaction based. For example, licence exception RPL is a licence exception that allows the one for one replacement of parts without the need for a licence from BIS for the transaction.

Licence exceptions often have conditions and limitations on their use. Part 740.2 of the EAR, which discusses licence exception conditions and restrictions in detail, should be consulted prior to any use of a licence exception to ensure use of the exception is permissible. Use of an exception where it is not permissible is a violation of the EAR.

Sometimes, licence exception conditions are noted in the ECCN of the item. Figure 2 above show one such limitation on the use of licence exception STA for ECCN 9A610. Companies must ensure that they understand the appropriate use of a licence exception before implementing its use for a particular re-export or retransfer.

Companies must also ensure that the licence exception's recordkeeping and reporting requirements are adhered to. The logic used to determine whether or not a licence exception applies to a particular item/transaction should be documented for each transaction.

It is best practice to document the rationale used to determine the licensing requirements or eligibility for use of a licence exception for each re-export or retransfer of an item subject to the EAR.

No Licence Required (NLR)

For some re-exports and retransfers, no licence is required (NLR). There are specific conditions that must be met for this to be the case.

There are generally two scenarios where one can re-export or retransfer an item subject to the EAR as NLR.

The first scenario is when an item is not listed on the CCL (it does not have an ECCN) but is still subject to the EAR (EAR99) AND general prohibitions (4-10) do not apply to the transaction. Refer to Part 736 of the EAR for the list of 10 General Prohibitions.

The second scenario is when an item is listed on the CCL (it has an ECCN) but does not require a licence to the destination (there is no "X" in the applicable Commerce Country Chart cell) AND general prohibitions (4-10) do not apply to the transaction.

These are the only two instances where NLR can be properly used. If the re-export or retransfer does not meet the requirements of NLR, then the company will need to

either obtain a licence from BIS or identify an applicable item based or transaction based licence exception prior to allowing the re-export or retransfer to take place.

The references at the end of this document under **Determining the applicable licensing requirements** may assist with licensing determination.

Making a Licence Application with BIS using SNAP-R

SNAP-R stands for Simplified Network Application Processing System – Redesign. It is the BIS on-line interface with industry. Through SNAP-R, industry can request classification advice and apply for export and re-export licences. Each Company has login credentials for SNAP-R and is responsible for creating and managing work items in accordance with its own policies and procedures. SNAP-R can be accessed through the BIS website, www.bis.doc.gov , or at www.snapr.bis.doc.gov/snapr . The SNAP-R system contains a user's manual with detailed instructions about how to use the system and complete the multipurpose application, form 748-P.

Creating a Work Item is the main activity in SNAP-R. There are five types of work items:

1. Export Licence applications
2. Re-Export Licence applications
3. Commodity Classification requests
4. Encryption Registrations
5. Agriculture Licence Exception notices

As Export Licence applications are only available for exports from the United States, Australian companies will primarily be using the Re-Export Licence application for all items subject to the EAR.

The other type of work item you may use is the Commodity Classification request. This work item is used to ask BIS for advice as to an item's applicable ECCN.

Prior to creating a work item, the user will have completed analysis on the commodity and transaction that includes:

For any work item:

- A determination as to whether the item is subject to the EAR
- A determination as to the applicable ECCN, or possibly applicable ECCN(s)
- Product/model number
- Quantity and value (per unit and total)
- Manufacturer
- Technical description (as related to parameters described in the ECCN) Prepare a 250 word summary.
- Available documentation to support the submission (technical specifications, brochures, etc.)

- End-use of the item
- Prior licensing of the item (was it supplied to [Company Name] under a DPS-5, GC, etc. or has the item previously been licenced for re-export by BIS) and the licence number where applicable
- Resubmission A C N, where applicable

Additional analysis required for a re-export application:

- End-users of the item
- Names and addresses of all consignees, including intermediate consignees
- Denied parties screening of all parties to the export transaction

The references at the end of this document under SNAP-R (Classification Advice, Licensing, Licence Tracking) may assist with making a licence application through SNAP-R: It is best practice for more than one user to have administrative rights to a work item in SNAP-R. There may be instances where an administrator must leave the office for a planned or unplanned period. For each work item, the assignment of a second user with administrative rights is critical in order for the organization to maintain the ability to manage work items in SNAP-R. Where an administrator's absence from the office is planned, administrative rights to work items can be temporarily granted to another person or trained employee. At the end of the administrator's absence, the administrative rights may be revoked.

Licence Exceptions

A Licence Exception is a special authorisation that allows you to export or re-export, under very specific conditions, items that would otherwise require an export licence. For a full listing of Licence Exceptions review EAR§740 available at www.bis.doc.gov.

By using any of the Licence Exceptions, you are certifying that the terms, provisions, and conditions for the use of the Licence Exception described in the EAR have been met. Each Licence Exception bears a three-letter symbol that will be used for export clearance purposes.

Your Export Declaration must record the correct Exception symbol (e.g., LVS, GBS, CIV) and the correct Export Control Classification Number (ECCN) (e.g., 4A003, 5A002) for all shipments of items exported under a Licence Exception.

Records of transactions involving exports under any of the Licence Exceptions must be maintained for five years at a minimum. Below is a summary of EAR Exceptions that are available, however, it is important that you review all of the associated requirements on www.bis.doc.gov.

Exception	Description
Shipments of Limited Value [LVS]	Authorises the export and re-export in a single shipment of eligible commodities.
Temporary Imports, Exports & Re-exports [TMP]	Authorises various temporary exports and re-exports; exports and re-exports of items temporarily in the U.S.; and exports and re-exports of beta test software.
Servicing / Replacement of Parts & Equipment (RPL)	Authorises exports and re-exports associated with one-for-one replacement of parts or servicing and replacement of equipment for previously exported equipment.
Governments, International Organisations (GOV)	Authorises exports and re-exports for international nuclear safeguards; U.S. government agencies or personnel, and agencies of co-operating governments; international inspections under the Chemical Weapons Convention; and the International Space Station.
Technology and Software (TSU)	Authorises exports and re-exports of operation technology and software; sales technology and software; software updates (bug fixes); “mass market” and encryption source code (and corresponding object code) that would be considered publicly available under the EAR.
Additional Permissive Re-exports (APR)	Re-exports from Country Group A:1 and co-operating countries.
Shipments to Country Group B countries (GBS)	Authorises exports and re-exports to Country Group B.
Civil End-Users (CIV)	Authorises exports and re-exports of items on the CCL that have a licence requirement to the ultimate destination pursuant to the Commerce Country Chart for NS reasons only.
Encryption commodities, software and technology (ENC)	Authorises export and re-export of systems, equipment, commodities and components therefor that are classified under ECCN 5A002.a.1, .a.2, .a.5, .a.6, .a.9, or .b, systems, equipment and components therefor classified under ECCN 5B002, and equivalent or related software and technology classified under ECCN 5D002 or 5E002.
Technology and Software Under Restriction (TSR)	Authorises exports and re-exports of technology and software where the Commerce Country Chart indicates a licence requirement to the ultimate destination for national security reasons only and identified by “TSR—Yes” in entries on the CCL.

Gift Parcels and Humanitarian Donations (GFT)	The provisions of paragraph (a) authorise exports and re-exports of gift parcels by an individual (donor) addressed to an individual, or a religious, charitable or educational organisation (recipient) located in any destination for the use of the recipient or the recipient's immediate family (and not for resale).
Computers (APP)	Authorises exports and re-exports of computers, including "electronic assemblies" and specially designed components therefor controlled by ECCN 4A003, except ECCN 4A003.e (equipment performing analog-to-digital conversions exceeding the limits in ECCN 3A001.a.5.a), exported or re-exported separately or as part of a system for consumption in Computer Tier countries.
Strategic Trade Authorisation (STA)	Exporters are able to export less sensitive military items without a licence to 36 countries if they meet the requirements of revised Licence Exception Strategic Trade Authorisation (STA).

Strategic Trade Authorisation (STA)

Under the STA exception, exporters are able to export less sensitive military items without a licence to 36 countries if they meet the requirements of revised Licence Exception Strategic Trade Authorisation (STA).

To qualify for the licence exception, the export has to be for one of three purposes, for:

- Ultimate end-use by a government of one of the 36 closest U.S. allies;
- Return to the U.S.; or
- Shipping under an existing licence issued by the U.S. government that authorises the use of Licence Exception STA.

To use Licence Exception STA, the export, re-export, or transfer must first meet all of the general Licence Exception STA requirements that apply to all items that are subject to the EAR. For example, the Export Control Classification Number (ECCN) of the item must specifically list STA as a possible licence exception. All other reasons for control that apply to the transaction must also be authorised. In addition, the exporter must provide the consignee with the ECCN, obtain a specific statement from the consignee, notify the consignee that the shipment is subject to Licence Exception STA, and keep a record showing which shipments belong to each consignee statement.

Note: Items exported under Licence Exception STA may not be re-exported under Licence Exception APR.

Prior Consignee Statement

The exporter, re-exporter and transferor must obtain the following statement in writing from its consignee prior to shipping the item and must retain the statement in accordance with part 762 of the EAR. One statement may be used for multiple shipments of the same items between the same parties so long as the party names, the description(s) of the item(s) and the ECCN are correct. The exporter, re-

exporter, and transferor must maintain a log or other record that identifies each shipment made pursuant to this section and the specific consignee statement that is associated with each shipment.

[INSERT NAME OF CONSIGNEE]:

3.1 Is aware that [INSERT DESCRIPTION AND APPLICABLE ECCN OF ITEMS TO BE SHIPPED] will be shipped pursuant to Licence Exception Strategic Trade Authorisation (STA) in § 740.20 of the United States Export Administration Regulations (15 CFR 740.20);

3.1 Has been informed of the ECCN noted above by [INSERT NAME OF EXPORTER, RE-EXPORTER OR TRANSFEROR];

3.1 Understands that items shipped pursuant to Licence Exception STA may not subsequently be re-exported pursuant to paragraphs (a) or (b) of Licence Exception APR (15 CFR 740.16(a) or (b));

3.1 Agrees not to export, re-export or transfer these items to any destination, use or user prohibited by the United States Export Administration Regulations; and

3.1 Agrees to provide copies of this document and all other export, re-export or transfer records (i.e., the documents described in 15 CFR part 762) relevant to the items referenced in this statement to the U.S. Government as set forth in 15 CFR 762.7.

STA Exception and the 600 Series

The STA exception is available for exports, re-exports, and in-country transfers of less sensitive military items under the new “600 series”. “600 series” items are, by definition, military items or items specially designed for military applications, Licence Exception STA is only available for these items under narrow circumstances. In addition, there are additional compliance obligations on exporters who want to use the STA licence exception. The following prerequisites must also be met to use Licence Exception STA for “600 series” items.

The export, re-export, or transfer has to meet one of the following three purposes:

3.1 The export must be for an ultimate end use by the U.S. government or a government of a country listed in new Country Group A:5 (STA-36 countries). These include all NATO countries, Australia, New Zealand, Japan, South Korea, and Switzerland.

3.1 The export must be for return to the U.S. (for example, the export of a “600 series” item for the Joint Strike Fighter (JSF) project in a STA-36 country, where the item or the end item will be returned to a JSF manufacturer in the U.S.).

3.1 The export must be for shipping under an existing licence issued by the U.S. government that authorises the use of Licence Exception STA.

3.1 Non-U.S. parties must have been previously approved on a licence issued by BIS or the U.S. Department of State, Directorate of Defence Trade Controls (DDTC).

The consignee statement must address the ultimate end user restrictions for “600 series” items and agree to permit a U.S. government end-use check with respect to the items.

Additional requirements apply to end item aircraft listed in ECCN 9A610.a, such as unarmed military aircraft and military helicopters. Exporters and other persons who intend to export, re-export, or transfer these items under Licence Exception STA may do so only after submitting a written Licence Exception STA eligibility request to BIS and obtaining BIS’s approval to use this licence exception. Applicants who receive an approval notification may share it with companies affiliated with them, such as a branch or distributor.

BIS has implemented a STA decision tool to help exporters determine if they are eligible to use Licence Exception STA [Search Google Strategic Trade Authorisation (STA) decision tool].

Companies that are planning to use Licence Exception STA, particularly for “600 series” items, will need to spend diligent attention to all of the requirements that follow this licence exception. This will require an initial investment to incorporate the notification, consignee statement, record-keeping, and other requirements into their existing export compliance processes and documentation.

The De-minimis Rule

If your item contains some U.S. technology, it is controlled for export and re-export by the U.S. Government for the life of that product. However, if the product contains less than a certain percentage of U.S. technology, the goods will not be controlled by the U.S. Government. However, you must remember that the country where you are exporting from will most likely require an export permit.

The following steps are provided as general guidance for determining whether a non-U.S. produced item (commodity, software, or technology) that incorporates U.S.-origin items/technology is subject to the EAR or is not subject to the EAR pursuant to the de minimis rules in the EAR. This general guidance does not take into account specific U.S.-origin items that are not eligible for de minimis treatment. You should consult Section 734.4 and Supplement 2 to Part 734 for information on such items and guidance on how to calculate the percentage of U.S.-origin controlled content.

If you are a company that incorporates U.S.-origin commodities in a commodity, you will need to:

- Determine the classification (ECCN) of the U.S.-origin commodities exported to you. The U.S. exporter may be able to assist you in determining the ECCN or you may submit a classification request to BIS via SNAP-R (no cost+).
- Determine if the U.S.-origin commodities are "controlled content." ("U.S. controlled content" is content that would require a U.S. licence if it were to be re-exported separately to the country of ultimate destination.)
- Determine if the percentage of U.S.-origin "controlled content" is greater than 25% of the value of your finished non-U.S. product. (For exports to designated terrorist supporting countries (Country Group E:1), you need to determine if the

U.S.-origin "controlled content is greater than 10% of the value of your finished product.)

- If the U.S.-origin controlled content is 25% or less of the value of your finished product (or 10% or less for terrorist supporting countries), your product is not subject.

If the U.S.-origin controlled content percentage is greater than 25% (or 10% for terrorist-supporting countries), your product is subject to the EAR. If your product is subject to the EAR, you need to determine if your item requires a licence, either because of the ultimate destination or the end-use or end-user.

Calculating De Minimis

Calculation of the value of controlled U.S.-origin content in non-U.S.-made items is performed to determine whether the percentage of U.S.-origin content is de minimis. However, you do not need to make these calculations if the non-U.S. made item does not require a licence to the destination in question. Use the following guidelines to perform such calculations:

U.S.-Origin Controlled Content

To identify U.S.-origin controlled content, you must determine the Export Control Classification Number (ECCN) of each U.S.-origin item incorporated into the product.

Then, you must identify which, if any, of those U.S.-origin items would require a licence from BIS if they were to be exported or re-exported (in the form in which you received them) to the non-U.S.-made product's country of destination. For purposes of identifying U.S.-origin controlled content, you should consult the Commerce Country Chart. Commodities subject only to short supply controls are not included in calculating U.S. content.

NOTE: U.S.-origin controlled content is considered ‘incorporated’ for de minimis purposes if the U.S.-origin controlled item is:

3. Essential to the functioning of the non-U.S. equipment;
3. customarily included in sales of the non-U.S. equipment; and
3. re-exported with the non-U.S. produced item.

Technology and source code used to design or produce non-U.S.-made commodities or software are not considered to be incorporated into such non-U.S.-made commodities or software.

Value of U.S.-origin controlled content

The value of the U.S.-origin controlled content should reflect the fair market price of the content in the market where the non-U.S. product is being produced. In most cases, this value will be the same as the actual cost to the non-U.S. manufacturer of the U.S.-origin commodity, technology, or software. If fair market value cannot be determined based upon actual arms-length transaction data for the U.S.-origin controlled content in question, then you must determine another reliable valuation method to calculate or derive the fair market value. Such methods may include the use of comparable market prices or costs of production and distribution. The EAR

does not require calculations based upon any one accounting system or standards. However, the method you use must be consistent with your business practice.

Non-U.S.-made product value

The value of the non-U.S.-made product shall reflect the fair market price of such product in the market where the non-U.S. product is sold. In most cases, this value will be the same as the actual cost to a buyer of the non-U.S.-made product. If fair market value cannot be determined based upon actual arms-length transaction data for the non-U.S.-made product in question, then you must determine another reliable valuation method to calculate or derive the fair market value. Such methods may include the use of comparable market prices or costs of production and distribution. The EAR does not require calculations based upon any one accounting system or U.S. accounting standards. However, the method you use must be consistent with your business practice.

Non-U.S.-Made Software

In calculating the value of non-U.S.-made software for purposes of the de minimis rules, you may make an estimate of future sales of that non-U.S. software. The total value of non-U.S.-made software will be the sum of the value of actual sales of that software based on orders received at the time the non-U.S. software incorporates U.S.-origin content and, if applicable; an estimate of all future sales of that software.

Note: Regardless of the accounting systems, standard, or conventions you use in the operation of your business, you may not depreciate reported fair market values or otherwise reduce fair market values through related accounting conventions. Values may be historic or projected. However, you may rely on projected values only to the extent that they remain consistent with your documentation.

Calculating percentage value of U.S.-origin items

To determine the percentage value of U.S.-origin controlled content incorporated in, commingled with, or “bundled” with the non-U.S. produced item, divide the total value of the U.S.-origin controlled content by the non-U.S.-made item value, then multiply the resulting number times 100. If the percentage value of incorporated U.S.-origin items is equal to or less than the de minimis levels then the non-U.S.-made item is not subject to the EAR.

One-time Reporting Requirement

A one-time report is required before reliance on the de minimis rules for technology. The purpose of the report is solely to permit the U.S. Government to evaluate whether U.S. content calculations were performed correctly.

You must include in your report a description of the scope and nature of the non-U.S. technology that is the subject of the report and a description of its fair market value, along with the rationale and basis for the valuation of such non-U.S. technology. Your report must indicate the country of destination for the non-U.S. technology re-exports when the U.S.-origin controlled content exceeds 10%, so that BIS can evaluate whether the U.S.-origin controlled content was correctly identified. The report does not require information regarding the end-use or end-users of the re-exported non-U.S. technology. You must include in your report the name, title,

address, telephone number, E-mail address, and facsimile number of the person BIS may contact concerning your report.

Submission of Report

You must submit your report to BIS using one of the following methods:

(1) E-mail: rpd2@bis.doc.gov

(2) Fax: (202) 482-3355; or

(3) Mail: Regulatory Policy Division, U.S. Department of Commerce, Bureau of Industry and Security, Regulatory Policy Division, Room 2705, 14th and Pennsylvania Avenue, NW, Washington, DC 20230.

Using De-minimis

If you have not been contacted by BIS concerning your report within thirty (30) days after filing the report with BIS, you may rely upon the calculations described in the report unless and until BIS contacts you and instructs you otherwise. BIS may contact you with questions concerning your report or to indicate that BIS does not accept the assumptions or rationale for your calculations. If you receive such a contact or communication from BIS within thirty (30) days after filing the report with BIS, you may not rely upon the calculations described in the report, and may not use the de minimis rules for technology until BIS have indicated that such calculations were performed correctly.

Record Keeping

While most records to be retained are outlined in Part 762.2(a) of the EAR, there are also record keeping requirements located throughout the regulations. Part 762.2(b) contains a list of references to 51 other sections of the EAR that contain records to be retained not listed in Part 762.2(a). As the EAR requires such a large variety of records to be retained, Export Control Officer (ECO) should refer to the list of documents (Part 762.3) that the EAR does not require industry to retain when creating EAR recordkeeping procedures at each business unit.

Records related to the licensing of an item subject to the EAR shall be retained for five (5) years from the date of expiration of the licence.

Where the transaction is eligible for use of a licence exception or is “NLR”, records related to the determination of NLR or licence exception eligibility shall be retained for five (5) years from the date of the transaction.

Project specific procedures and requirements on record retention and archiving may require extended record retention periods for some items and transactions.

The EAR contains regulations on the manner in which documentation should be managed where records are maintained electronically. The EAR has specific requirements related to electronic recordkeeping practices:

1. All records may be kept electronically, provided they can be readily accessed, reproduced onto paper and are readable. (Section 762.5)

2. Where records are kept electronically, the company must have written procedures to identify individuals who are responsible for the use, operation and maintenance of recordkeeping systems (Section 762.5(b)(5))

   AND

- The company must establish written procedures for inspection and quality assurance of records in the system and document the implementation of those procedures (Section 762.5(b)(6))

  AND

- The company must provide a method for correlating, identifying and locating records relating to the same transaction(s) that are kept in other record keeping systems. (Section 762.5(b)(7))

  AND

- The company must record where, when, by whom, and on what equipment the records and other information were entered into the system) (Section 762.5(b)(8).

The system must be able to locate and reproduce all records relating to a particular transaction based on any one of the criteria listed in section 762.5(c)):

(1) The name(s) of the parties to the transaction;

(2) Any country(ies) connected with the transaction; or

(3) A document reference number that was on any original document.

Voluntary Self-Disclosure

BIS encourages the submission of Voluntary Self Disclosures (VSD) by parties who believe they may have violated the EAR. VSD are an excellent indicator of a party's intent to comply with U.S. export control requirements and may provide BIS important information on other ongoing violations. BIS carefully reviews VSD received from disclosing parties to determine if violations of the EAR have occurred and to determine the appropriate corrective action when violations have taken place. Most VSD are resolved by means other than the issuance of an administrative penalty. Of the VSD received and resolved in Fiscal Year 2005, 97% were resolved either with a finding that no violation of the EAR had occurred (55%) or with the issuance of a warning letter (42%). Of VSD received and resolved in Fiscal Year 2006, 100% were resolved either with a finding that no violation of the EAR had occurred (52%) or with the issuance of a warning letter (48%). In instances in which BIS determines that the issuance of an administrative penalty is appropriate for the resolution of a VSD, BIS affords the submission of a VSD "great weight" in assessing and mitigating the penalty. In appropriate cases, fines and other administrative penalties may be significantly reduced.

Submitting a Voluntary Self-Disclosure

One copy of the information constituting a VSD or any other correspondence pertaining to a VSD may be submitted to:

Director, Office of Export Enforcement (Check name of incumbent)
1401 Constitution Ave.
Room H4514
Washington, DC 20230
Tel: (202) 482-1208
Facsimile: (202) 482-5889

Annex E: Pro Forma Technology Control Plan

Begins on next page

[ITAR] Technology Control Plan (TCP)

Version [01] dated [insert date]
FOR
[insert project/product description] (the "Program")

ADHERENCE TO THE PROCEDURES DESCRIBED IN THIS TCP AND OTHER [Company name] POLICIES GOVERNING THE TRANSFER OF ITAR MATERIAL **IS MANDATORY** FOR ALL PERSONNEL INVOLVED IN THE PROGRAM

[Company Name] Entity:
[insert name of company establishing the TCP]
hereinafter referred to as "[Company Name Abbreviated]"

Technology Control Officer (TCO): [insert name]
Export Control Officer (ECO): [insert name]

Abstract

Mandatory Technology Control Plan containing procedures and control measures to ensure compliance with ITAR requirements in relation to controlled technical information. Nevertheless, its strongly recommended to write a general TCP in other cases. This template can be simplified to suit the situation, especially in academic institutions and smaller companies.

TCP CONFIGURATION CONTROL

TCP VERSION	DATED	ISSUED BY	REASON FOR ISSUE
01	DRAFT		Original Document
02	DRAFT		Updated draft
03			

TABLE OF CONTENTS

DEFINITIONS

The following words and expressions, as used in this TCP shall have the following meanings:

CECC	*Commodity Export Classification Certificate*[or an equivalent certificate that certify's the classification of a supply by the supplier]
DDTC	The US Department of State Directorate of Defense Trade Controls
Defense Article	Any item designated on the United States Munitions List (USML).
Defense Services	(i) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; or (ii) The furnishing to foreign persons of any Technical Data, whether in the United States or abroad, or (iii) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad, or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise and military advice. (Defined in ITAR paragraph §120.9)
DSP	A US export licence form bearing the signature of DDTC and a licence number and issue date.
ECO	The Export Control Officer identified on the front of this TCP. The ECO is the [Company Name] employee primarily responsible for management of export procedures for the [Company Name] entity listed on the front of this TCP.
Foreign	Non-United States
ITAR	International Trafic in Arms Regulation
ITAR Material	Any Technical Data or Defense Services
ITAR Material Register	The register to be maintained by the TCO in the form set out in Appendix D.
NDA	A non-disclosure agreement in the form set out at Appendix G.
Licence	Any US export licence needed to export ITAR Material from the US, including without limitation, TAAs, MLAs and DSPs
NDA	Non-disclosure agreement
TAA/MLA	Technical Assistance Agreements/Manufacturing License Agreements
TCO	The Technology Control Officer identified on the front of this TCP.
TCP	This ITAR Technology Control Plan

Technical Data	• information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of Defense Articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation; • classified information relating to Defense Articles and Defense Services; • information covered by an invention secrecy order; and (iv) software directly related to defense articles. Note: This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain as defined in ITAR paragraph § 120.11. It also does not include basic marketing information on function or purpose or general system descriptions of Defense Articles. (Defined in ITAR paragraph §120.10). The term Technical Data includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in the USML. It does not include basic marketing information on function or purpose or general system descriptions. (Defined in ITAR paragraph §120.6.)
USML	United States Munitions List as defined in Part 121 of the ITAR

PURPOSE

The International Traffic in Arms Regulations (ITAR) are a set of United States government regulations that control the export and re-transfer of US defence materials, and associated technology (referred to as ITAR Material) to non-US countries, companies, or individuals.

Under the ITAR, any US party wishing to export or transfer ITAR Material to any non-US entity or person must obtain advance authorisation from the US State Department through the DDTC. DDTC authorisation is also required for any “re-exports” of ITAR Material, where a recipient of ITAR Material wishes to transfer it to a different party, end-use or destination. This means that a company intending to receive ITAR Material needs to implement an organisation and measures for securing and controlling transfers of such ITAR Material.

The purpose of this TCP is to detail the organisation and controls implemented by [Company Name] to secure and control transfers of ITAR Material within the Program; to comply with the terms of the TAA/MLA signed in relation to the Program; and to ensure that no transfer of ITAR Material occurs unless duly authorised by the DDTC.
The procedures and controls contained in this plan apply to all [Company Name] personnel involved in the Program.

References

This TCP should be read in conjunction with the following [Company Name] Corporate Export Control processes: [Example policies]

Reference	Document Title	Version
1	Standard of Export Compliance	
2	Guidelines to ensure compliance with regulations applicable to outsourced items	

3	Contratheque Guidelines for ITAR Agreements	
4	Export Control Reference Guide	
5	Commodity Export Classification Certificate (CECC)	
6	Model procedure for responding to potential export control violations	
7	Export control : Declaration procedure in relation to nationalities rule under US ITAR 124.16	

TECHNICAL ASSISTANCE AND MANUFACTURING LICENSE AGREEMENTS (TAA/MLAS)

Technical Assistance Agreements and Manufacturing License Agreements are the main mechanisms for non-US entities to receive US Technical Data and/or US Defense Services and engage in technical discussions of the ITAR Material. These agreements are the formal US export authorisation to cover the performance of Defense Services and / or the disclosure of ITAR Material by the US supplier and require DDTC approval before coming into effect. They are generally accompanied by a number of provisos (restrictions) relating to the use of the ITAR Material. TAAs and MLAs are subject to US laws, including notably ITAR, and legal sanctions may be applied to both companies and individuals in the event of any non-compliance. A summary of the TAA(s)/MLA(s) to which this TCP relates is attached at Appendix A.

RESPONSIBILITIES OF TCO

It is the role of the TCO to :

- ensure that only Program personnel duly authorized are given access to ITAR Material
- nominate the authorised [recipients/points of entry] for ITAR Material in the Company and inform the US exporter(s) of ITAR Material to the Company, in writing of such authorised [recipients/points of entry] for ITAR Material in the Company
- ensure that any ITAR Material received in the Company, other than by an authorised recipient is immediately quarantined pending an investigation as to whether the actual recipient has the right to receive it and why the proper transmission channels were not followed
- record details of all ITAR Material properly received in the Company in the ITAR Material Register
- ensure that ITAR Material received by [Company Name] is not further transferred, transmitted, shipped, mailed, hand-carried (or delivered by any other means of transmission) unless a U.S. export authorization allowing the transmission has already been obtained by [Company Name] and the transmission procedures follow the requirements of the export authorization and is performed with the prior approval of the ECO

- make individuals participating in the Program aware of all regulations concerning the right to access, the handling and safeguarding of the ITAR Material
- brief all relevant employees on the contents of the TCP and to ensure that they execute a TCP Briefing Acknowledgement Form in the form set out in Appendix C. Copies of all such briefings and acknowledgement forms are to be retained by the TCO for audit purposes
- ensure that the following documents are completed, as applicable, and maintained accurately and in an up to date manner, in the form set out in the relevant Appendix to this TCP:
    - TCP Briefing Acknowledgement Form (Appendix C)
    - ITAR Material Receipt/Transfer Register (Appendix D)
    - ITAR Material receipt acknowledgement form (Appendix E)
    - List of Authorised ITAR Program Personnel (Appendix F)

AUTHORISED PERSONNEL

As soon as a TAA/MLA has been signed by all Parties, and a TCP issued, the TCO shall complete the list of Authorised Program Personnel, identifying, by name, all personnel authorized to handle the ITAR Material. This list shall form part of the TCP Briefing to ensure that everyone working on the Program is aware of those personnel duly authorized to receive the ITAR Material.

Prior to adding an employee's name to the List of Authorised Personnel, the TCO shall verify with HR that that employee is authorised to receive ITAR. When this has been confirmed, the TCO shall enter the details of such person on the form set out in Appendix F and shall maintain this register for the period of the Program, ensuring that it is kept up to date at all times and any person no longer working on the Program is removed immediately.

RECEIPT OF ITAR MATERIAL

Immediately upon receipt, all ITAR Material shall be entered into the ITAR Material Register held by the TCO. All fields shall be completed in relation to each item of ITAR Material received.

Any person, other than the TCO, receiving the ITAR Material shall promptly inform the TCO of its receipt with sufficient details to allow the TCO to record the receipt in the ITAR Material Register.

Tangible ITAR Material must be placed in a document storage wallet clearly marked as follows (regardless or whether the document is marked as being ITAR controlled):

"***WARNING - Information Subject to US Export Control Laws***

The document(s) in this folder contain information subject to the International Traffic in Arms Regulations (ITAR). Only persons authorised in writing by [INSERT NAME OF TCO] may open this folder. Any other person opening this folder may be subject to disciplinary action and US criminal sanctions. This information may only be exported, released, or disclosed in accordance with TAA Ref: [ ] and may not be exported, released, or disclosed to unauthorised parties without prior written approval from the US State Department ".'

When ITAR Material is generated or re-transferred in written or other physical form (e.g. documents, drawings, computer tape, video tape, e-mail, CD, or other storage media.) the following warning must be placed on the front cover or other appropriate location (e.g. header and/or footer) of each such document or storage media to prohibit improper re-transfers to persons not authorised to receive the data:

'***WARNING - Information Subject to US Export Control Laws***

This document contains information subject to the International Traffic in Arms Regulations (ITAR). This information may only be exported, released, or disclosed in accordance with TAA Ref: [ ] and may not be exported, released, or disclosed to unauthorised parties without prior written approval from the US State Department.'

In addition, ITAR 123.9(b) requires the following statement to be included on all invoices and bills of lading/airway bill relating to the ITAR Material:

"WARNING: These commodities are authorized by the USG for export only to [country of ultimate destination] for use by [end user] under [license or other approval number or exemption citation]. They may not be resold, diverted, transferred or otherwise be disposed of, to any other country or to any person other than the authorized end user or consignee(s), either in their original form or after being incorporated into other end-items, without first obtaining approval from the U.S. Department of State or use of an applicable exemption.

RECEIPT OF UNMARKED ITAR MATERIAL

In the event that any material is received which is not marked as subject to ITAR but there is any ambiguity or doubt regarding whether or not it could be ITAR Material, clarification should be sought immediately from the ECO who will quarantine the ITAR Material as necessary. ITAR marking will normally be found on the associated invoices, packing lists and on technical data.

GENERATION OF TECHNICAL DATA

During the course of the Program, [Company Name] may be required to generate technical data in order to support its obligations under the Program. It is recognised that some of the data generated under the Program may incorporate ITAR Material supplied by the customer and / or sub-contractors and as such may be subject to ITAR control (and other export control restrictions).

When producing such data, it is the responsibility of the individual generating the technical data to make a preliminary assessment of the information contained therein, to identify:

- whether the information is subject to security classification in accordance with any written instructions provided by the customer. Security classification of any material must be verified by the Security Controller.

and;

- whether any of the information contained within the data is either ITAR controlled or could be deemed to be technical information which may require export approval. Classification of any material as export controlled must be verified by the ECO.

Following verification of classification by the Security Officer/Controller and/or ECO as the case may be, the individual should mark the document in accordance with the requirements.

Any ITAR controlled data generated must also be added to the ITAR Material Register and will be subject to the same controls, including as to rights of access, as ITAR Material received from the US supplier .

DATA CONTROL

All ITAR Material received or generated by [Company Name] personnel shall be held at the relevant company premises authorised under this TCP in a secure cabinet or, if in electronic form, on a stand alone secure hard drive or server only accessible to those authorised by the DSP/TAA/MLA and identified on the List of Authorised ITAR Project Personnel. The TCO shall maintain a written record of all access to and transfers of ITAR Material in a 'Transfer of ITAR Material Record' document in the form set out in Appendix D . This includes access by [Company Name] personnel and all transfers to third parties (which must be made only with the prior approval of the ECO, who will verify whether such transfer is authorised under the DSP/TAA/MLA). For each access or transfer, the following information must be recorded:

- to whom the access was granted or to whom the transfer was made;
- the precise ITAR Material accessed/transferred;
- on what date the access/transfer took place;
- the general subject matter of the access/transfer in a generic form readable by those not covered by the DSP/TAA/MLA.
- A countersignature by the individual recipient against each entry.

ITAR MATERIAL – SEGREGATED WORKS AREA

All ITAR Material is to be held and used in an access controlled area to prevent any potential access by unauthorised personnel.

[Describe how ITAR material is received and allocated to the concerned Program]

US CLASSIFIED DATA

[Text to be added on TAA/MLA-by-TAA/MLA basis to cross refer to any specific requirements in the TAA/MLA (Attachment 1) re transmission, treatment of Classified or other Protectively Marked Information.]

DATA RETURN/DESTRUCTION

Text to be added on TAA/MLA-by-TAA/MLA basis

[Note: At the conclusion of a TAA/MLA, a US Applicant may request that the company either return all ITAR Material to the US Applicant, or may instead request that the company destroy the data. but don't forget about your own recordkeeping requirements]

SUB-LICENSING

(i.e. re-transfer of ITAR Material to further permitted recipients/categories of recipients, e.g subcontractors). N.B. Sublicensees have authority to receive ITAR Material, but they do not have authority to interact/discuss this information with the US Applicant or any other US parties

[*Sub-Licensing is not permitted under the TAA/MLA*].

[*Sub- Licensing is permitted to the following parties: [Here list details from TAA/MLA of permitted sub licensees and their roles and the defence articles or data permitted to be transferred to each]*]

[*delete as appropriate*]

RETRANSFER REQUESTS

Where ITAR Material needs to be transferred to any party not nominated on the original DSP 5 licence, a retransfer authorization request **must** be submitted and approved by the US Department of State BEFORE any movement of the ITAR Material is made. The model covering letter and retransfer request is set out in Appendix H and must be completed in full by the ECO.

It is extremely important to ensure that necessary information is included with the request since this can otherwise cause rejection of the request. Such information should include a purchase order issued to [Company Name] and an End User Statement, both from the customer (not necessarily the End User), as well as a product brochure, and copies of previous export licenses. Copies of acceptable end user statements to be provided are attached at Appendix I.

AUDIT

The « Program » must occasionally be subject to an audit by the internal/external auditors. Moreover, the « Program » must do self-evaluation in order to identify areas needing to be improved and to underline the strengths of export compliance program. All potential violations of this TCP will be treated according to Corporate directives. [*delete as appropriate*]

The TCO must develop a corrective action plan if necessary in order to deal with unresolved action as quickly as possible. The following self-evaluation must include terminated corrective actions.

POINTS OF CONTACT

Any queries regarding this document or the process to be adopted should be addressed to the following:

Name	[ ]
Position	TCO
Phone Number	[ ]
E-Mail Address	[ ]

Name	[ ]
Position	ECO
Phone Number	[ ]
E-Mail Address	[ ]

APPENDIX A

[Note: A separate sub-Appendix for each TAA/MLA is to be prepared]

TAA/MLA Summary

A copy of the TAA/MLA and any provisos relating thereto/summary of provisos relating thereto to be attached to this Appendix.

Note: The summary below is not intended to be a substitute for reading the entire agreement. It is important to read the agreement to ensure full understanding of all obligations.

Summary of TAA / MLA

TAA Case No [insert] / MLA Case No: [insert]]

Parties: [insert names]

Date of TAA/MLA: [ ]

Expiry Date of TAA/MLA: [ ]

Permitted Purpose: [insert directly from TAA/MLA**]**

The authorisation granted for use of the ITAR Material applies only to the ITAR Material expressly defined within the TAA/MLA for the Permitted Purpose only.

If any other ITAR Material is received or any other use is proposed, immediate contact should be made with the local ECO. [Note re handling of non-authorised ITAR Material]

Authorised nationalities:

This authorisation applies to employees of [Company Name(s)] who are nationals of the following countries:

Eg United Kingdom
Dual nationals from the list at (iii) below
Third party nationals from any of the countries listed below:

NATO
Belgium, Bulgaria, Canada, Czech Rep, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, United States;

EUROPEAN UNION
Austria, Belgium, Bulgaria, Cyprus (Greek part), Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom;

OTHER COUNTRIES
Australia, Japan, New Zealand , Switzerland and South Korea.

Note that for the purposes of the authorisation under this section, all access and/or re-transfers of ITAR Material to employees of a Party from the above countries must take place completely within the physical territories of the above countries or the United States; and

Execution of an Individual Non-Disclosure Agreement (I-NDA) is NOT required for dual national and/or third country national employees from these countries.

[Countries marked with "NDA" additionally require an NDA to be executed prior to any disclosure of ITAR Material. The form of this NDA is attached at Appendix G.]

Third party dual nationals holding both nationalities from countries listed above
Note: For the purpose of this authorisation. "employee" means:
Permanent employees of any of the Parties
[and Contract labour employees of the parties to the TAA/MLA (hired directly or indirectly)];

[insert any further categories of authorisation/authorised nationalities under the TAA/MLA (e.g. where an Individual Non-Disclosure Agreement (I-NDA) is required)].
[delete as appropriate]

All access and/or retransfers must take place completely within the physical territories of these countries or the United States. Note that in addition to the requirements of this TCP that all shipments of ITAR material must be made with the prior approval of the ECO.

TAA/MLA Limitations and Provisos:

[Insert any other limitations and requirements contained in the TAA/MLA]

APPENDIX B

TCP Briefing Templates

Company specific templates such as powerpoint, briefs or notes.

APPENDIX C

TCP Briefing acknowledgement form

[Company Name] Technology Control Plan (TCP) Version [ ] dated [ ]

for

[*insert project/product description*]
(the Program)

I, _____(*insert name of individual*) confirm that I have been briefed by _____(*insert name of TCO*) on the contents of this TCP, I have received a copy of the TCP and I acknowledge and understand the requirements of this TCP.

_____
Print name

_____
Signature

_____
Date

APPENDIX D

ITAR Material Register Receipt/Transfer Form

Version [insert version no] dated [insert date]

Date of entry	Serial No/ Document Ref	Date ITAR Material Received by authorised person	Transferor	Recipient	Description	Location (where it is stored)	Media (Paper/ CD etc)	Relevant Licences (e.g. DSP 5; TAA etc)	Comments	Signature of TCO

APPENDIX E

ITAR MATERIAL RECEIPT ACKNOWLEDGMENT FORM

Type of Material:	Technology/Physical item*
Description of item/technology to be transferred:	
Part No:	
ECCN No:	
Technical Assistance Agreement (TAA) /Licence ref and date (Copy or summary to be attached):	

I, the undersigned, acknowledge that, prior to receipt of the above mentioned ITAR Material, I have received a copy of the above TAA/Licence* relating to the ITAR Material described above.

I confirm that I have read and understood the terms and conditions of such TAA/Licence* and agree to comply with such terms and conditions in relation to the ITAR Material above mentioned.

I further undertake that I shall ensure that I shall not transfer the ITAR Material to anyone who is not duly authorized to receive it under the TAA/Licence* and then only after such duly authorized person has agreed to be bound by the terms and conditions of the TAA/Licence* by completing and executing another example of this ITAR Material Transfer form.

Signed:……

Name:……

Job title:…….

Domain: ……

Name of line manager: ……

Date:……..

Attachments: Technical Assistance Agreement*
US Export Licence*

* Delete as appropriate

In the event of any doubt in relation to the obligations placed by signature of this document, please contact your Export Control Department.

APPENDIX F

List of Authorised Personnel [form]

Project:

TAA/MLA Ref:

Names of Personnel Authorised for Access to/Use of ITAR Material

Name	Department/Location

APPENDIX G

Non-disclosure Agreement

I, _____, acknowledge and understand that any technical data related to defense articles on the U.S. Munitions List, to which I have access or which is disclosed to me under this license by [company name] is subject to export control under the International Traffic in Arms Regulations (Title 22, Code of Federal Regulations, parts 120-130). I hereby certify that such data will not be further disclosed, exported or transferred in any manner, to any other foreign national or any foreign country without the prior written approval of the Office of Trade Controls Licensing (DDTC), U.S. Department of State.

_____
Print name

_____
Signature

_____
Date

APPENDIX H

Model Form of Retransfer Authorisation Request Letter

The following letter is to be submitted to the [Company Name] Trade Compliance team (trade.compliance@email address), who will place it on Corporate letterhead and submit it to the DDTC for authorisation on behalf of the company. This template should be modified to suit the purpose.

Example Model Letter to be completed:

PLEASE SEND AUTHORISATION LETTER
BY FEDEX (ACCT NO. 4818-5494-6) TO:
[Joe Blowe]
Trade Compliance Manager
[Company Name], Inc.
[Address Line 1]
[Address Line 2, Country, Post Code]

[DATE]

[Mr. Kevin Maloney] – Check current incumbent]
Director, Office of Defense Trade Controls Licensing
Directorate of Defense Trade Controls
U.S. Department of State
PM/DDTC, SA1, 12th Floor
2401 E. Street, N.W.
Washington D.C. 20037

PMDDTC Code: M-14512

Subject: Retransfer Authorization Request (ITAR § 123.9(c))
[PRODUCT] [INCORPORATED INTO [PRODUCT]] for Retransfer to [COUNTRY]

USML Category: Category [NUMBER AND DESCRIPTION]

Dear Mr. Maloney:

On behalf of [Company Name], a company located in [CITY, COUNTRY], [US Subsidary if appropriate], requests authorization to permanently [OR TEMPORARILY] retransfer unclassified USML Category [NUMBER] [PRODUCT] [INCORPORATED INTO [PRODUCT]] to [COUNTRY] for use by [WHOM].

The [PRODUCT] was originally exported from the U.S. under DSP–5 License No. [NUMBER] for [PURPOSE (i.e., INTEGRATION INTO A PRODUCT)]. The end-use for these items remains unchanged

[OR DESCRIBE NEW END USE]. The [PRODUCT] is a [DESCRIBE PRODUCT IN TERMS OF FUNCTION AND/OR ITS ROLE IN THE END ITEM]. It is manufactured from [MATERIAL]. [ETC.]

In support of this request, we have attached summary details on the proposed retransfer at Tab A [INCLUDING A COPY OF THE ORIGINAL EXPORT LICENSE]; a [PRODUCT] product brochure at Tab B; a copy of the [PURCHASE ORDER] [LETTER OF INTENT] [CONTRACT] at Tab C; and a [STATEMENT BY THE End-User (SEE TAB C FOR EXAMPLE)] identifying the [END USER] as the end-user at Tab D.We appreciate your urgent attention to this retransfer request. Should you have any questions or require additional details, please contact me at (703) 519-6318, or by e-mail at [Joe.Blowe]@[Company Name].com. Please forward your final response to us by Federal Express (Account Number xxxxxxx) to the attention of Mr Joe Blowe, [Company Name], Inc., [Address].

* * *

I am a responsible official empowered by the applicant, [Company Name], to certify the following in compliance with ITAR § 126.13:

4. Neither [Company Name], its chief executive officer, president, vice presidents, other senior officers or officials, nor any member of its board of directors is the subject of an indictment for or has been convicted of violating any of the U.S. criminal statutes enumerated in ITAR § 120.27 since the effective date of the Arms Export Control Act, or is ineligible to contract with, or to receive a license or other approval to import defense articles or defense services from, or to receive an export license or other approval from, any agency of the U.S. Government.

5. To the best of [Company Name]'s knowledge, no party to the export as defined in ITAR § 126.7(e) has been convicted of violating any of the U.S. criminal statues enumerated in ITAR § 120.27 since the effective date of the Arms Export Control Act, or is ineligible to contract with, or to receive a license or other approval to import defense articles or defense services from, or to receive an export license or other approval from, any agency of the U.S. Government.

* * *

Sincerely,

[Joe Blowe]
Trade Compliance Manager
Empowered Official

U.S. Exporter and Authorizations:

[PRODUCT NAME (IF MORE THAN ONE)]

[NAME]
[ADDRESS]

DSP-5 License No. [NUMBER]

Quantity: [NUMBER]
Value for each: $[VALUE]
USML Category: [NUMBER]

[REPEAT FOR EACH COMPONENT]

Purchaser:
[NAME]
[ADDRESS]

End-User:
[NAME]
[ADDRESS]

Intermediate Consignee:
[NAME]
[ADDRESS]

Final Platform:
[PRODUCT]

Program & Quantity:
This retransfer request covers [QUANTITY] [PRODUCT] [INTEGRATED INTO [PRODUCT]]

Total Retransfers:
[QUANTITY] [PRODUCT]
[REPEAT FOR EACH COMPONENT]

Value of Items Subject to Retransfer:
$[TOTAL VALUE OF ALL COMPONENTS RETRANSFERRED]

ATTACHMENTS:

Product brochure
Purchase order/letter of intent/contract
End User Statement

APPENDIX I

Model forms of End User Statements

End Use and End User. Applicant must seek written confirmation from the foreign purchaser before applying for a license. The license application must include from the foreign customers a written statement regarding the specific end-user and end user. This information may be included in the purchase order/contract or in a separate document. When the end use and end user confirmation is provided in a separate document, the document must identify the referenced purchase order/contract. (Excerpt from guidelines for DSP-5 completion instructions)

Example of end user statement contained on P.O./Contract/Letter of Intent:

"The [PRODUCT] is to be [INTEGRATED INTO [Company Name] [PRODUCT] and] further integrated [by [DIRECT UNIT CUSTOMER]] into [FINAL PLATFORM] for use by [END USER]. The [PRODUCT] is being procured from [Company Name] by [CUSTOMER] pursuant to purchase order [CONTRACT] number [NUMBER]. The [FINAL PLATFORM] is being procured from [CUSTOMER] by [END USER] pursuant to purchase order [CONTRACT] number [NUMBER].

Signed,"

[END USER] *Best Option*
[CUSTOMER] *Alternative, but not guaranteed to meet State Department Requirements*

Alternatively, the End User could complete a separate document, such as the one on the following page or another format that identifies all of the parties to the transaction, the ITAR controlled item, the end user, the end use, etc.

Example of separate End User Statement

[TO BE PLACED ON CUSTOMER'S LETTERHEAD]

To: [Company Name]
[FULL ADDRESS]

From: [CUSTOMER]

Re: P.O./Contract/Letter of Intent No.: _____

Date: [DATE]

We understand that the product(s) requested under the above referenced P.O./Contract/Letter of Intent may require licensing from the United States Government prior to shipment. In order to assist [Company Name] in making this determination and obtaining an export license, if required, we are providing the following information:

1. Equipment to be exported, including part number and description.

   [PLEASE ELABORATE IN DETAIL. IN ADDITION TO HARDWARE, LIST ANY DOCUMENTATION OR TECHNICAL SUPPORT REQUIRED (I.E. TRAINING OR INSPECTION). USE AN ATTACHMENT, IF NECESSARY.]
   _____
   _____

2. The ultimate end user of the product(s) is:

   [PROVIDE NAME AND ADDRESS, INCLUDING AGENCY, DIVISION]
   _____
   _____

3. The name of the program or platform the product(s) will be used in is:
   _____
   _____

4. The specific purpose for the export is:

   [FOR EXAMPLE: INCORPORATION INTO A SYSTEM, ASSEMBLY, TESTING, AND EVALUATION. PROVIDE AS MUCH DETAIL AS POSSIBLE.]
   _____
   _____

5. The name, address, and role of each party that will receive your product(s) prior to delivery to the ultimate end user are:

   [FOR EXAMPLE: ASSEMBLY HOUSE, PRIME CONTRACTOR, SALES AGENT, FREIGHT FORWARDER. USE AN ATTACHMENT, IF NECESSARY]
   _____
   _____

Signed, etc.

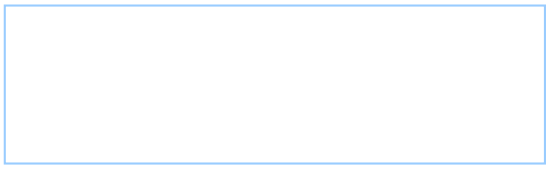
Annex E-1: Project/Site Technology Control Plan

Begins on next page.

[COMPANY NAME]
Address
Zip Code, Town
Country
Tel.: +00 (0) 00 00 00 00
Fax: +00 (0) 00 00 00 00
www.xxxxxxxxxx.com

PROJECT TECHNOLOGY CONTROL PLAN

THIS IS THE [COMPANY NAME] PROJECT SPECIFIC TECHNOLOGY CONTROL PLAN FOR XXXX PROJECT



Follow-up of the evolutions/versions

LOG OF CHANGES			
Revision	**Date**	**Author**	**Modification**
001			
002			
003			

APPROVAL				
	Name	**Role**	**Date**	**Signature**
Written by				
Verified by				
Approved by				
Approved by the customer if necessary				

CONTENTS

LIST OF TABLES

LIST OF FIGURES

PURPOSE

The purpose of this Project TCP is to detail the procedures and controls implemented by [enter site and project name here] to secure and control transfers of ITAR Material within the Project; to comply with the terms of the TAA/MLA signed in relation to the Project; and to ensure that no transfer of ITAR Material occurs unless duly authorised in accordance with the [Company Name] Technology Control Plan. The procedures and controls contained in this plan apply to all personnel involved in the Project.

REFERENCES

This Project TCP should be read and used in conjunction with the following [Company Name] processes:

Reference	Document Title	Version
1	[Company Name] Technology Control Plan	Insert hyperlink
2	Security Self Inspection and Reporting Instruction	

TAA/MLA OR OTHER EXPORT AUTHORISATIONS AND DOCUMENTATIONS

All relevant project TAA/MLA and/or Third Party Retransfer Authorisations details are recorded in a summary within this Project TCP along with a full copy of all agreements. The summary includes all details on parties to the agreement, sub-licensees and any specific limitations.

The authorisation applies only for the purpose defined within the TAA/MLA for this project.

If any ITAR Material is proposed to be used for another purpose outside of this project, a separate authorisation will be required. This can be sought through the ECO.

TAA/MLA Summary

A copy of the TAA/MLA and any provisos relating thereto/summary of provisos relating thereto to be attached to this Summary.

Note: The summary below is not intended to be a substitute for reading the entire agreement. It is important to read the agreement to ensure full understanding of all obligations.

Summary of TAA / MLA [insert]

TAA Case No [insert] / MLA Case No: [insert]]

Parties: [insert names]

Date of TAA/MLA: [ ]

Expiry Date of TAA/MLA: [ ]

Permitted Purpose: [insert directly from TAA/MLA]

The authorisation granted for use of the ITAR Material applies only to the ITAR Material expressly defined within the TAA/MLA for the Permitted Purpose only.

If any other ITAR Material is received or any other use is proposed, immediate contact should be made with the local ECO. [Note re handling of non-authorised ITAR Material]

AUTHORISED PERSONNEL

A complete list of all personnel authorised IAW with the [Company Name] Technology Control Plan to handle the ITAR Material is maintained in this Project TCP.

This list forms part of the TCP Briefing to ensure that everyone working on the Project is aware of those personnel duly authorised to receive the ITAR Material.

Prior to adding an employee's name to the List of Authorised Personnel, the TCO shall verify that that employee is authorised to receive ITAR. The company TCP defines what an ITAR Authorised person is through the Trade Control Authorisation Instruction. All completed copies of the Trade Control Authorisation Instruction are attached to this Project TCP following the List of Authorised Personnel.

The TCO shall maintain this register for the period of the Project, ensuring that it is kept up to date at all times and any person no longer working on the Project is removed immediately.

List of ITAR Authorised Personnel

Name	Position	Means of Authorisation (Clearance or TCAI)

PROJECT TCP BRIEFING AND ACKNOWLEDGEMENT

All project personnel who are ITAR Authorised have been briefed on the contents of this Project TCP and the relevant TAA/MLA. As such a copy of their briefing and acknowledgement form is held within this Project TCP.

Project TCP Briefing Acknowledgement Form

Project Technology Control Plan (TCP) Version [ ] dated [ ]

for

[*insert project/product description*]
(the Project)

I, _____(*insert name of individual*) confirm that I have been briefed by

_____(*insert name of TCO*) on the contents of this

Project TCP, I have reviewed a copy of the Project TCP and I acknowledge and understand the requirements of this Project TCP.

_____
Print name

_____
Signature

_____
Date

RECEIPT OF ITAR MATERIAL

An ITAR Material Register that contains a list of all ITAR Material received by the Project is maintained within this Project TCP.

The TCO is responsible for maintaining the register. Any person, other than the TCO, receiving ITAR Material shall promptly inform the TCO of its receipt with sufficient details to allow the TCO to record the receipt in the ITAR Material Register.

ITAR Material Register Receipt/Transfer Form

Version [insert version no] dated [insert date]

Date of entry	Serial No/ Document Ref	Date ITAR Material Received by authorised person	Transferor	Recipient	Description	Location (where it is stored)	Media (Paper/ CD etc)	Relevant Licences (e.g. DSP 5; TAA etc)	Comments	Signature of TCO

RECEIPT OF UNMARKED ITAR MATERIAL

In the event that any material is received which is not marked as subject to ITAR but there is any ambiguity or doubt regarding whether or not it could be ITAR Material, clarification should be sought immediately from the ECO who will follow the instructions IAW the [Company Name] TCP. Until this clarification has been received, the suspected US material must be treated as ITAR controlled. ITAR marking may normally be found on the associated invoices, packing lists and on technical data.

ITAR INTEGRATION INTO PROJECTS

Any ITAR controlled items integrated by the project into project material or data must also be added to the ITAR Material Register within this Project TCP by the TCO and will be subject to the same controls, including access, storage and re-transfer as other ITAR material.

STORAGE OF ITAR MATERIAL

All ITAR Material received or generated by [Company Name] personnel shall be held within the relevant ITAR Storage Area (ISA) designated by the Project TCO and site Security Officer, which adherers to the Physical Storage requirements of the company TCP and is only accessible to those identified on the List of Authorised ITAR Project Personnel within this Project TCP. Tangible ITAR Material must be clearly marked as per the directions in the company TCP.

ITAR STORAGE AREA (ISA)

The ISA(s) for [Insert Site and Project Name] are/is located as follows:

[Insert site, room and other relevant details for the ISA here]

Example ONLY (please delete once above is completed):

The ISA for Project XXXX at [location] is located in the separate caged area within the warehouse adjacent to the workshop. The area is signed as ITAR STORAGE AREA and can only be accessed by ITAR authorised personnel listed in this Project TCP.

DESTRUCTION AND DISPOSAL OF ITAR CONTROLLED TECHNOLOGY

When the ITAR material is no longer required by the project, it is either returned to the provider with appropriate receipts of its return or it is destroyed using suitable means IAW the [Company Name] TCP.

The ITAR/EAR Destruction Form must be used and fully completed to provide evidence of destruction IAW “Instruction on destruction of ITAR and EAR controlled items”.

A copy of any destruction forms are kept within this Project TCP.

AUDITS

Audits are conducted by the TCO IAW with the [Company Name] TCP.

POINTS OF CONTACT

Any queries regarding this document or the process to be adopted should be addressed to the following:

Name	[ ]
Position	Business Unit / Site / Project TCO
Phone Number	[ ]
E-Mail Address	[ ]

Name	[ ]
Position	Business Unit / Site / Project ECO
Phone Number	[ ]
E-Mail Address	[ ]

T 1300 55 66 77 W aigroup.com.au E info@aigroup.com.au