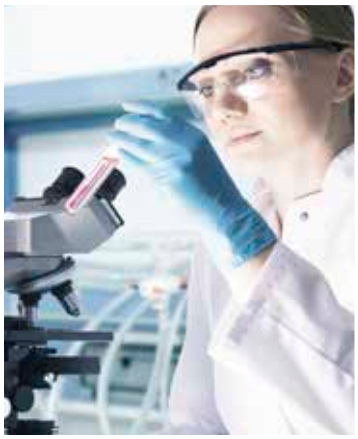
Australian Best Practice Guide for the management of controlled exports and technology

AUSTRALIAN INDUSTRY GROUP








Australian Best Practices Guide for the Management of Controlled Exports and Technology

A general guide for transactions outside the Australia U.S. Treaty on Defence Trade Cooperation's 'Approved Community' Arrangements.

Last updated: May 2014

AUSTRALIAN INDUSTRY GROUP

DISCLAIMER: This Guide has been developed by the Best Practices Working Group of the Australian Export Control Forum. The information contained herein is not intended to be relied upon as legal opinion and does not constitute, in any manner, legal advice. All information is provided 'as is' and is subject to change. The authors of this Guide do not assume any legal liability or responsibility for the accuracy and completeness of the information herein.

Acknowledgements:

The Guide has been developed by the Best Practices Working Group of the Australian Export Control Forum. Working Group participants included;

Jason Brown – Thales Australia (Chair)
Eva Galfi – International Trade Advisors (Editor)
Tony Antoniades – BAE Australia (formerly of Thales Australia)
Julia Reed – Australian Aerospace (formerly of Boeing)
Michael Hughes - Raytheon

The Group would like to acknowledge the assistance with from relevant government agencies in the development and review of the Guide.

The foundations of this guide were researched and developed by Adelaide Jones of as part of her internship with Thales and her degree course at the University of Canberra National Security Institute.

Table of Contents

Introduction

The Export Control Forum's Best Practices Working Group created this guide with the hope that it will serve as a resource to Small and Medium Enterprises (SMEs) in the understanding of their obligations and the development of corporate export compliance programs.

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

To assist Australian SMEs in understanding their legal obligations, Part One of this guide provides general information about managing export controlled goods and technology including;

- an overview of Australian export controls,
- a brief overview of United States export controls,
- an overview of U.S. export control reform,
- an overview of the Australia US Defence Trade Cooperation Treaty (the Treaty),
- information on the application of the U.S. ITAR's dual and third country national policy.
- the consequences of violating export control legislation,

Part Two of this guide provides examples of 'best practices' for managing controlled exports and technology. It was developed through interviews and the solicitation of written submissions from compliance managers at Australian prime contractors.

While the Working Group recognises that resource and budget constraints may make it difficult for SMEs to implement complex compliance programs, we hope that Part Two 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.

Part One – General Information About Controlled Exports and Technology

Section A – General Information about Controlled Exports

- Overview of Australian export controls
- Why are export controls important?
- Who in Industry / Business should be concerned about export controls?
- Key Government Organisations involved in Australian export controls
- Overview of US export controls
- US export control reform
- Overview of the Australia US Treaty on Defence Trade Cooperation
- Considerations for dual and third country nationals
- Penalties for Violations

Overview of Australian Export Controls

The ***Customs Act 1901*** and Regulation 13E of the ***Customs (Prohibited Exports) Regulations 1958*** control the export of defence and dual use goods in Australia. The **Defence and Strategic Goods List (DSGL)** identifies goods which Regulation 13E prohibits from being exported from Australia without a license or permit. 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 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 licenses to the Defence Export Control Office (DECO). DECO is responsible for reviewing export license applications and granting export permits and licenses. Information and further guidance about the process of applying to DECO for an export license or permit can be found on the DECO website.

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

In late 2012, the ***Defence Trade Controls Act 2012*** received royal assent. It implements the Australia U.S. Defence Cooperation Treaty (the Treaty) and

introduces provisions to strengthen existing export controls by regulating the intangible supply of controlled technologies on the DSGL, such as supply by electronic means; and brokering the supply of DSGL goods and technology. However many of its provisions had not come into effect at the time this guide was written, including the Act's offence provisions. There is a two year phased transition period for the provisions to come into effect. This means that exporters are not required to seek permission to supply DSGL-listed technology intangibly or to broker its supply until the Minister for Defence issues a proclamation to that effect. Check the Defence Export Control Office website for the latest advice (www.defence.gov.au/deco).

A consultation draft of the ***Defence Trade Control Regulation 2013*** was released in February of 2013. In addition to outlining the requirements for becoming an Approved Community member under the Treaty, these regulations create recordkeeping requirements for the intangible supply of controlled technologies and the brokering of controlled goods and technologies.

The **Customs Amendment (Military End-Use) Bill** was passed in November of 2012. It amends the *Customs Act 1901* to allow the Minister for Defence to prohibit exports that would or may be for a military end-use that would prejudice the security, defence or international relations of Australia. As this amendment is a 'catch-all', prohibition power, there is no need for exporters to apply for permits under this section of the Customs Act. While a permit is not required, it is recommended that exporters should undertake due diligence in any foreign trade to ensure the legitimacy of any export and if an exporter suspects an export may be for a military end-use that might be contrary to Australia's defence, security or international relations, they should contact DECO for assistance.

The **Weapons of Mass Destruction (Prevention of Proliferation) Act 1995** provides for the control of exports of 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 assist a WMD program. If you have at any time any reason to believe or suspect that your goods or services will or may be used in a weapons of mass destruction program you need to immediately advise DECO. You must not proceed with the export or supply of goods, or the provision of services, without first discussing the reasons for the belief or suspicion with DECO.

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.

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.

Why are export controls important?

Australia as a nation, and the companies which operate in Australia for the purposes of importing and/or exporting defence or dual-use technology, seek to meet a range of important obligations and responsibilities including;

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

Who in Industry / Business should be concerned about export controls?

Export controls are a concern for everyone. Adherence to corporate export control policies and procedures is incumbent upon every member of a company's staff, permanent or temporary, and in particular those who have export management and/or export compliance responsibilities.

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.

Key Government Organisations involved in Australian export controls:

The Australian Customs and Border Protection Service

- Facilitates legitimate trade
- Maintains border control of goods and passengers
- Verifies that export and import permits have been obtained prior to the cross border movement of goods
- Has monitoring powers
- Responsible for enforcement and compliance

The Department of Defence

- Administers legislation for control of defence and dual use goods and issues export licenses and permits
- Defence Export Control Office (DECO)- Acts as a liaison between government and industry through their website and outreach program

The Department of Foreign Affairs and Trade (DFAT)

- Formulates trade policy
- Represents Australia internationally at export control regimes
- Administers sanctions

The Australian Federal Police

- Investigation and prosecution powers

Overview of US Export Controls

The U.S. controls all exports. Exports of military goods and technology, as well as goods and technology that have a 'dual use' and can be put to military or civilian applications, will in most cases require an export license. This includes intangibles such as information contained in emails or communicated over the telephone.

The International Traffic in Arms Regulations and the Export Administration Regulations

The U.S. Government views the sale, export, and re-transfer of defense articles and defense services as an integral part of safeguarding U.S. national security and furthering U.S. foreign policy objectives. Authorizations to transfer defense articles and provide defense 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 cognizant of the potentially adverse consequences of indiscriminate arms transfers and, therefore, strictly regulates exports and re-exports of defense 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 defense articles and defense services from the US. The AECA charges the US 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 defense 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. Defense 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.

The EAR is administered by the United States Department of Commerce, **Bureau of Industry & Security (BIS)**. The Export Administration Regulations (EAR) govern 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's Commerce Control List (CCL). The CCL can be found in Supplement 1 to part 774 of the EAR. 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 then 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 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)s 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.

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.

US controlled technology governed by ITAR or EAR in your company's possession may be listed in via of the following:

- Technical Assistance Agreements;
- Manufacturing License Agreements;
- Warehouse and Distribution Agreements;
- DSP 5 – Licence for permanent export of unclassified defense articles and related technical data listed on the USML;
- Commerce Department licenses issued by the Bureau of Industry and Security for items subject to the EAR;
- Foreign Military Sales Contracts; and
- other US Government agency (e.g. US Nuclear Regulatory Commission and the Department of Energy, and Department of the Treasury) export licences or export arrangements.

Your company also retains documentation with respect to the application of the *de minimus* rule when planning to export items of non-US origin that may be considered subject to the EAR.

The **AECA** is the cornerstone of US law governing the export of military goods and technology. The U.S. Department of State implements the AECA by administering the **ITAR** through their Directorate of Defence Trade Controls (DDTC). The DDTC is responsible for reviewing license applications and granting export licenses for the movement of goods, services, and technology controlled by the ITAR's U.S. Munitions List (USML).

Dual use goods and technology are governed by a different set of laws and regulations. The **Export Administration Act of 1979** (currently expired and temporarily enforced though the **International Emergency Economic Powers 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's Bureau of Industry and Security (BIS). BIS is responsible for reviewing license applications and granting export licenses for the movement of goods and technology controlled by the EAR's Commerce Control List (CCL).

In many instances the Australian Government has acquired ITAR controlled U.S. defence equipment and technical data via Government to Government arrangements, this is known as **Foreign Military Sales (FMS)**. Under U.S. requirements associated with export control of FMS articles, it is only the Commonwealth 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 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.

Various other U.S. agencies, such as the Nuclear Regulatory Commission and the Department of Energy, and Department of the Treasury, also have licensing authority for exports.

Exemptions and Exceptions to licensing requirements

The ITAR offers exporters certain *exemptions* to licensing requirements, which allow for the export without a license of certain goods and technology, provided the strict conditions of the exemption are met. Similarly, the EAR offers exporters certain *exceptions* to its licensing requirements. The use of ITAR exemptions and EAR exceptions require that the exporter has a clear understanding about the export transaction and the product to ensure that the conditions of the exemption or exception can be met. In addition, detailed records must be kept to demonstrate that the export was eligible for use of the exemption or exception. Exporting goods under an exemption or exception erroneously is tantamount to exporting without an export license and can result in fines, penalties, and in some cases jail time for wilful violators.

US Export Control Reform

Over the course of the past few years, the U.S. has been undertaking a reform of its export controls in order to both better protect the crown jewels of U.S. military technology and make it easier for U.S. allies, including Australia, to access dual use and military items.

As the reforms progress, Australian industry can expect changes to the way U.S. goods and technology are categorised and licensed. As of April 2014, thirteen of the twenty one categories on the ITAR's US Munitions List (USML) have been revised. The revision has resulted in a reorganization of these ITAR categories and the movement of a significant number of articles from the USML to the Commerce Control List (CCL), which is governed by the provisions of the U.S. Export Administration Regulations (EAR). This change in jurisdiction will result in key changes to the way in which Australian industry manages these assets. Some key considerations include:

- Goods and technology previously controlled under the ITAR being controlled by the EAR; making familiarity with the EAR's requirements increasingly important for Australian companies.

- Goods and technology previously licensed by the US Department of State will now be licensed by the US Department of Commerce. In order to ensure that the appropriate US government approvals can be obtained in advance of the need to re-export or retransfer items subject to the ITAR or EAR, it is important for Australian industry to know which items in their possession or care will be changing jurisdiction and when the change will occur.

- 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 USML controlled. Special rules regarding licensing requirements, exception usage, recordkeeping, and reporting requirements apply to 600 series items.

- Non-U.S. Companies are authorised to make their own determinations of changes to the classification of goods and technology post U.S. export control reform. The U.S. exporter and/or OEM is 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 license or may be eligible for export without a license under an EAR license exception. However, the US 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 companies exporting or receiving EAR controlled items under a license exception.

- Australian companies may apply to the BIS for Commerce Department licenses to export, re-export, retransfer EAR controlled items. Australian companies can apply for both classification advice (Commodity Classification Request) and licenses (Re-export licenses) 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 license applications. Further information can be found at https://snapr.bis.doc.gov/snapr/

- Grandfathering provisions may apply to some State Department-approved export licenses and ITAR Agreements for up to two years after the items listed on these approvals have changed jurisdiction. However, these provisions are only designed to afford industry more time to make the procedural and commercial changes required to comply with the change in jurisdiction. After grandfathering provisions expire, TAAs, MLAs, WDAs will need to be re-baselined to include only ITAR controlled articles.

- All categories on the ITAR's USML are being rewritten and re-organised and new categories created. As a result, USML classifications assigned pre-reform are now either incomplete or incorrect. All USML classifications will need to be reviewed in the face of reform and corrected.

- Many key terms and definitions in both the ITAR and EAR have been revised. All revised and new definitions apply across the ITAR and EAR as of the effective date of the legislative change.

- The record keeping provisions of the EAR are much more detailed and require the retention of significantly more documentation than the ITAR. Details about the EAR's record keeping requirements are outlined in Part 762 of the EAR, but can be found in other sections as well when record keeping requirements relate to certain types of transactions. In addition, the EAR has specific reporting requirements for certain ECCNs and the use of certain license exceptions.

Further information about US export control reform, including progress of the reform effort and status of the reassignment of classifications and jurisdiction, can be found on the website of the US Department of Commerce's Bureau of Industry and Security (BIS) or the Export Control Reform website. (http://export.gov/ecr/index.asp).

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 update within 48 hours of legislative changes coming into effect.

Overview of the Australia US Defence Trade Cooperation Treaty

Readers of this guide should note the development of the Australia US Treaty on Defence Trade Cooperation (the Treaty) which will provide a framework for managing the export and transfer of defence goods and services (both classified and unclassified) between Australia and the US for 'Approved Community' members.

Approved Community members of the Treaty will not be required to apply for an export license from either the U.S. or Australian Governments to trade certain eligible goods, technology and services with other Approved Community members.

Further information about the Treaty can be found on Defence US Trade Treaty website (Link 1 in Annex 2).

Considerations for 'Dual and Third Country Nationals'

Background

Australia does not restrict access to Australian defence technology on the basis of nationality or country of birth. However, the U.S. Department of State considers these factors when assessing company employee access in license applications and agreements for the movement of ITAR controlled goods. As Australia imports over 50% of its military hardware from the US, the issue of employee nationality is important to Australian companies trading, storing or servicing ITAR controlled goods and technology.

Access to US Defence technology under ITAR has long been a complex issue. Under the ITAR, an employee's citizenship is only a part of the consideration that Australian companies must make. Companies must consider both nationality and citizenship when evaluating whether to grant access to an ITAR controlled article to a particular employee.

In addition to citizenship, the U.S. Department of State also considers, for the purpose of the ITAR, the individual's country of birth when determining what nationalities they hold. *Nationality* in the ITAR considers country of birth as well as citizenship.

> A person who migrated to Australia from Germany in the 1950's and became an Australian citizen in 1965 (relinquishing their German citizenship at this time) is considered under Australian law to be an Australian national only. Whereas, for the purpose of accessing US defence technology, the individual is considered to be a dual-national of both Germany and Australia. Under this scenario, either an explicit approval for German nationals or a licence exemption would normally be required for this individual to access US defence technology under the ITAR.

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 that was holds citizenship from one or more foreign countries in addition to their Australian citizenship.

In Australia, access has traditionally been limited to individuals who hold Australian citizenship unless other nationalities (country of birth, second citizenship) were specifically exempted or approved under a U.S. Department of State licence or agreement.

The U.S. Department of State requires that, in order for any dual or third country nationals to access ITAR controlled technology, an authorisation must first be obtained from the DDTC. Complicating the above issue is a US Government requirement that access to ITAR controlled technology is generally denied to individuals that are nationals of certain, 'proscribed' countries such as China, North Korea, Syria, Cuba, Iran and a number of other countries listed in ITAR 126.1. From time to time, countries are added or removed from the proscribed country list.

In the past, there was a presumption of denial of access to ITAR controlled technologies by citizens with ties to proscribed countries. Australians with a dual nationality from a proscribed country were generally not authorised to access ITAR controlled technology. The EAR has a different view of dual and third country nationals. The EAR does not consider country of birth for license applications. Only the current county of citizenship and/or country of permanent residency are regarded as relevant factors by the BIS. The BIS has issued extensive guidance on how their view of dual and third country nationals can be interpreted by companies administering controls to protect both ITAR and EAR controlled goods and technology. This guidance is available on the BIS website.

Using Exemptions

In 2011, the US Department of State released a new rule on "Dual and Third Country Nationals Employed by End Users", also known as ITAR exemption 126.18. This exemption and exemption 124.16 were made with the intent of reducing the administrative and compliance burden on foreign (Australian) end-users of ITAR controlled technology. These ITAR exemptions apply to regular employees of Australian companies that are considered to be 'dual and third country nationals'. The exemptions create broader access rights for *unclassified* ITAR controlled material in cases where the exemptions' specific requirements are met. There has been no change to access to classified ITAR controlled articles and technology.

Licence applications submitted by a US exporter to the US Department of State must seek specific approval for all dual and third country nationals that the Australian party anticipates will require access to ITAR controlled US technology or articles. This approval is obtained by either listing the specific nationalities, or by including a broad approval endorsed within the ITAR (e.g. the 124.16 exemption). If it becomes necessary to provide such access to a foreign national, including a dual-national, after an export licence has been approved by the Department of State, the US exporter must be notified so that they may request a licence or agreement amendment. ITAR exemptions 124.16 and 126.8 additionally allow for industry self-vetting of employees where conducted in accordance with guidance from DDTC. Additional

guidance on use of the industry self-vetting process is available on the DECO website.

Where a Technical Assistance Agreement (TAA) or a Manufacturing Licence Agreement (MLA) exists with a US company for the provision of services or manufacturing capability, dual and third country national access exemptions can be listed within the Agreement. There are various options/clauses available to Australian companies under TAAs/MLAs that can be requested when seeking access by their and their sub-licensees' dual and third country national employees. These include:

- Access to unclassified US defence technology where the individual holds an Australian Government security clearance, regardless of country of birth (ITAR Section 126.18 (c) (1)).
- Access to unclassified US defence technology through a screening process conducted by the employer to determine the risk of diversion of technology (ITAR Section 126.18 (c) (2)).
- Access to unclassified technology by specific identification of the nationalities within the TAA or MLA (by inclusion of an ITAR 124.8(5) statement).
- Access to unclassified technology to individuals from NATO, the European Union, Australia, Japan, New Zealand and Switzerland (ITAR 124.16).
- Access to *classified* US defence technology where the individual holds an appropriate Australian security clearance. For classified U.S. technology, there are still proscribed country limitations on the country of birth or dual-nationality of the individual. This exemption can only be used when the Commonwealth of Australia is a Party to the Agreement or the end-user.
- Access to classified technology by specific identification of the nationalities within the TAA or MLA (by inclusion of an ITAR §124.8(5) statement).

As a general rule, it is not necessary for export authorisations to identify each dual or third country foreign national by name. However, the Department of State can require the names of individuals holding a particular citizenship to be listed.

Where required by the associated exemption, dual and third country nationals may be required to sign a Non-Disclosure Agreement (NDA).

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, DWA) where they do not meet the conditions of exemption

124.16 or 126.18 (c) (1). The US exporter is required to keep NDAs for five years after termination of the agreement.

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 US. 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 license, license 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 the Defence Export Control Office is authorised to sign the foreign government certification block on the DSP-83.

Exports under a DSP- 5 license 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:

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

2. 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.

3. approval for accessing the ITAR controlled article(s) on the DSP-5 license 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.

Australia's Racial Discrimination Act and the ITAR

Access to ITAR 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 county of birth. However, the requirements of the ITAR may dictate that the employer do just that to meet the obligations of a license 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 Exemptions 124.61 and 126.18 may provide an appropriate avenue for avoiding such potential discrimination.

Penalties for Violations

Both the Australian and US export control regimes have a range of penalties for failure to follow their regulatory requirements. 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:

- Being placed on one of the US '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 American 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 in the public eye can be significant.

Penalties for violation of Australian export controls

The **Customs Act 1901** provides penalties for persons and/or companies who unlawfully attempt to export controlled goods without a permit or licence. The unlawful export of controlled goods, as specified in the DSGL, constitutes a tier 2 offence and could be subject to a fine not exceeding 2,500 penalty units or imprisonment for up to 10 years, or both. In addition, the goods as well as a conveyance used for the unlawful export of the goods may be seized and forfeited to the Commonwealth.

The **Defence Trade Controls Act 2012 includes offence provisions with imprisonment for up to 10 years, and** also makes it an offence to breach a condition of an export permit. The penalty for such a breach is 60 penalty units. Penalty Units are defined in section 4AA of the Crimes Act 1914 and are currently valued at $170 per penalty unit (as at February 2013) for a federal offence.

The Weapons of Mass Destruction (Prevention of Proliferation) Act 1995 (WMD Act) imposes substantial criminal penalties for breaching the prohibitions on the supply of tangible and intangible goods and services that may contribute to a WMD program. Criminal penalties of up to eight years imprisonment can be imposed for breaching the WMD Act.

Under the **Criminal Code Act 1995**, there are penalties for giving false information when applying for a permit or licence. A person who knowingly makes a statement to a Commonwealth entity that is false or misleading may

be prosecuted for an offence against the *Criminal Code Act 1995* and, if convicted, faces a penalty of up $12,000 and/or imprisonment for two years. A corporation faces a penalty of $60,000.

Penalties for violation of U.S. export controls

The scope and nature of penalties for violating US export controls is both significant and vigorously enforced. US 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 the United States, the following legislation and penalties can apply:

- Violation of the ITAR: Criminal penalties can reach 10 years imprisonment for individuals, including company officers, directors and employees, and $1,000,000 fine for each violation. Civil penalties can reach $500,000 per violation.
- Violation of the EAR: Criminal penalties can reach 20 years imprisonment and $1,000,000 for each violation. Administrative penalties can reach the greater of $250,000 per violation or twice the amount of the value of the transaction that is the basis of the violation.

Companies can also be debarred and have their export privileges suspended or revoked as a consequence of violating the EAR or ITAR.

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.

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. (Link 2, Annex 2)

Section B – General Information about Controlled Technology

- What is controlled technology?
- What is a deemed export?

What is controlled technology?

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

Technology can be stored electronically, recorded onto media, contained in emails or communicated over the telephone. Export controls are imposed on the technology by either the Commonwealth of Australia or foreign governments.

Technology is controlled to reduce global arms proliferation and protect arms technology from misuse by terrorist organizations and countries that are non-signatories to the Wassanaar Arrangements, Missile Technology Control Regime, or other multilateral regimes and arms control treaties.

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 (DECO) 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, this intangible supply will be regulated by the *Defence Trade Controls Act 2012* (the Act). However, during the two-year transition period, the offence provisions in Part 2 of the Act do not apply, and permits will only be required once a proclamation is issued by the Minister for Defence.

U.S. Controlled Technology: Under the ITAR, 'Technical Data' is defined in 120.10:

a) *Technical data* means, for purposes of this subchapter:

> (1) Information, other than software as defined in §120.10(a)(4), 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 or documentation.

(2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;

(3) Information covered by an invention secrecy order; or

(4) Software as defined in §121.8(f) of this subchapter directly related to defense articles.

(b) The definition in paragraph (a) of this section 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 §120.11 of this subchapter. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

The EAR also controls certain technologies, including technical data, and has its own definition of 'technology' in Part 772. In addition, in some instances the physical item may be controlled by the EAR 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 domestically is controlled.

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:

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

A license 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.

Part Two - Current Best Practices for companies in Australia

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.

Section A- Export Control Management Systems

Companies engaged in the import and export of controlled goods and technology need a comprehensive export control management system that ensures compliance while maintaining efficient business practices.

An Export Control Management System (ECMS) is a key part of a company's Internal Compliance Program (ICP). An ECMS will help to ensure that:

- the company's policies on export controls are clearly communicated,
- appropriate procedures are followed to safeguard the movement and export of export controlled goods and technology
- audits are regularly conducted to verify and improve compliance with legislation
- responsibilities for export control compliance are clearly outlined and employees are trained, as required
- resources for staff with questions about export policies and procedures are provided
- export controlled goods are not inadvertently sold or exported without proper screening of end users and required permits or licenses in place

Verification of compliance with export controls should be part of every step of the export process, from taking an order to the physical export of the good or technology.

Best practices for an ECMS include:

- Having a clear company policy on export controls and make export control compliance part of company risk review procedures in the corporate ICP.

- Designating an employee responsible for administering the ECMS, answering export compliance related questions and making decisions

about the ability for the company to export particular goods and technology on a transaction by transaction basis

- Implementing an audit plan to regularly assess the effectiveness of the ECMS and identify issues that have a negative impact on compliance

- Designating an annual budget for implementing, monitoring and improving the ECMS

- Requiring customers to complete a questionnaire to help assess export compliance risks prior to orders being accepted

- Implementing an annual training program to teach employees about the importance of export controls and the consequences to the company and to them personally of committing a violation

Internal Compliance Program Documentation

DECO has developed the following documents to assist companies in setting up and implementing an internal compliance program (ICP), 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.

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

Supply Chain Security

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 Authority's transport planning guidance for classified material (Link 3, Annex 2) or the alignment to the ISO 28000 Supply Chain Security Standard are useful templates for developing a company's transport policy and procedures.

Section B- Managing Controlled Technology

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
The measures in the **Defence Trade Controls Act 2012** introduce 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 introduces a number of new criminal offences to enforce the new provisions. 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. As indicated earlier, introduction of many of these additional enhanced Australian controls will be implemented over a two year transition period.

A Technology Control Plan is a key element of an Export Control Management System. The purpose of a TCP is to describe specific procedures for how access to classified and controlled unclassified information will be controlled to prevent unauthorised access. A TCP helps to ensure that controlled goods and technology are managed in compliance with legislative requirements and within the parameters of domestic and foreign export authorizations which govern their exports, re-exports or re-transfers.

Technology Control Plan (TCP) Elements

A comprehensive TCP should specify what constitutes controlled technology, outline governance arrangements, and describe the export management systems of the company. The TCP 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 and mandating compliance with the requirements of export controls
- Identification of facilities and premises to which the requirements apply
- Identification of company personal to whom the requirements apply
- The company's engagement with export should be clearly articulated
- Relevant requirements, processes and procedures should be articulated
- 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
- Responsibility for the management of export controls should be fully described, including providing 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 and mandated
- Model agreements and licences should be provided for reference
- Guidance on access to IT systems, to prevent unauthorised transfer of controlled technology, should be described and mandated
- Physical and personal security practices to prevent unauthorised access should be described and mandated. Including:
    - Access control
    - Visitor identification and control
    - Badging
    - Recruitment practices
    - Termination of employment
    - Security education and awareness training
    - Document and Data Storage
    - Recording
    - Transport
    - Disposal

- All export and import processes, including intangible transfers, should include review and documentation procedures to prevent unauthorised transfer at each key stage
- A grading and classification system should be described and in place
- Procedures for document control and handling should be adequately described.

A sample TCP is available in Annex 3 to this guide.

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.

Laptop Computers:

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

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

Best practices

- Don't send export controlled files by email or embed export controlled data in email text. Send links to internal pages that require a secure login.

- Don't 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.

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.

Best 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;
- An up-to-date list of all personnel authorised to access the nominated folders should be regularly provided to IT by the Technology Control Officer.
- 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 (Link 4, Annex 2) or the Information Security Manual published by the Defence Signals Directorate (Link 5, Annex 2).

ITAR Controlled Information

All information relating to ITAR-controlled technology that is stored electronically must be protected from unauthorised persons. Australian primes have detailed policies and procedures in place to safeguard ITAR controlled technology. Below is an excerpt from the policies and procedures of an Australian prime, outlining their requirements for accessing, transmitting and transferring ITAR controlled technology:

Electronic Storage of Information relating to U.S. ITAR-Controlled Technology.

The following rules shall be adhered to by all personnel with respect to data relating to ITAR-controlled technology:

- 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.

Transfer or Transmission of Information relating to 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 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;

- 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 2 business days, or any shorter time considered reasonable in the circumstances, the sender shall notify his/her local party responsible for corporate technology control.

Useful Resources

Australian Resources

Key legislation and the DSGL:

For an electronic copy of the **Australian Customs Act 1901** visit:
http://www.austlii.edu.au/au/legis/cth/consol_act/ca1901124/

The **Defence Strategic Goods List (DSGL)** can be found at
http://www.defence.gov.au/deco/DSGL.asp

You may find the **Quick Reference Guide** a useful tool to help you locate items in the DSGL. http://www.defence.gov.au/deco/DSGLQRG.asp

Customs (Prohibited Exports) Regulations 1958
http://www.comlaw.gov.au/Series/F1996B03403

Defence Trade Controls Act 2012
http://www.comlaw.gov.au/Details/C2012A00153

Key Australian Government Agencies

Department of Defence:

Defence Export Control Office (DECO):
www.defence.gov.au/deco
Phone: 1800 66 10 66 (+61 2 6266 7222)
Email: deco@defence.gov.au

US Trade Treaty Team
www.defence.gov.au/ustradetreaty
Phone: 1800 00 57 57 (+61 2 6265 7111)
Email: ustradetreaty@defence.gov.au

Australian Customs and Border Protection Service:
www.customs.gov.au
Phone: 1300 363 263
Email: information@customs.gov.au

U.S. Resources

Key legislation and control lists:

For the **Export Administration Regulations**, visit www.ecfr.gov and select Title 15, then Part 730 to 774. The **Commerce Control List (CCL)** is part 774 of the EAR. An electronic copy can be found on the eCFR website.

For the **International Traffic in Arms Regulations**, visit www.ecfr.gov and select Title 22, then Part 120 to 130. The **US Munitions List (USML)** is Part 121.1 of the ITAR. An electronic copy can be found on the eCFR website.

Key U.S. Government Agencies

DDTC Response Team
http://www.pmddtc.state.gov/response_team/index.html
Phone: (202) 663 1282 (Washington D.C.)
DDTCResponseTeam@state.gov

Bureau of Industry and Security (BIS):
www.bis.doc.gov
Phone: +1 202 482 4811 (for the Washington DC Office of Exporter Services)
Email available through an on-line form

Other Useful Resources

For updated information on the progress of **U.S. Export Control Reform**, visit www.export.gov/ECR

For guidance from the regarding the elements and implementation of an effective **Export Compliance Management Program**, visit http://www.bis.doc.gov/complianceandenforcement/emcp.htm.

For general information on **ITAR compliance requirements**, visit http://www.pmddtc.state.gov/.

For general information regarding **U.S. trade sanction programs**, visit http://www.treasury.gov/offices/enforcement/ofac/.

For information regarding **Australia's sanction programs**, visit http://www.dfat.gov.au/un/unsc_sanctions/

For assistance with ITAR issues, Australian companies can contact the Defence Industry Innovation Centre: www.enterpriseconnect.gov.au or call 131 791.

Export Controls Consultants in Australia

Centre for Export Controls Excellence (CFECE)
www.cfece.com
Office 2, Level 1
23-25 Bulcock Street
Caloundra
Ph: +61 (0)7 5314 2016
Mob: 0407 373 227

International Trade Advisors
www.internationaltradeadvisors.com.au
119 Willoughby Rd
Crows Nest NSW 2065
Eva Galfi's Mobile: 0421 506 095

Annexures

Annex 1: Acronyms used in this document

AECA – Arms Export Control Act (U.S.)

BIS – Bureau of Industry and Security (U.S.)

CCL – Commerce Control List (U.S.)

DECO – Defence Export Control Office (Australia)

DDTC – Directorate of Defense Trade Controls (U.S.)

DFAT – Department of Foreign Affairs and Trade (Australia)

DOC – Department of Commerce (U.S.)

DoD – Department of Defence (Australia)

DSGL – Defence and Strategic Goods List (Australia)

DSP- Department of State Publication

EAR – Export Administration Regulations (U.S)

ECMS – Export Control Management System

FMS – Foreign Military Sales

MLA – Manufacturing License Agreement

NDA – Non Disclosure Agreement

ICP – Internal Compliance Program

ITAR – International Traffic in Arms Regulations (U.S.)

RDA – Racial Discrimination Act (Australia)

SMEs – Small and Medium Sized Enterprises

TAA – Technical Assistance Agreement

TCP – Technology Control Plan

TPR – Third Party Retransfer

USML – United States Munitions List (U.S.)

VPN – Virtual Private Network

WDA – Warehouse or Distribution Agreement

WMD –Weapons of Mass Destruction

Annex 2: List of Links Referenced in this document

Link 1
Australia United States Defence Trade Cooperation Treaty:
http://www.defence.gov.au/ustradetreaty/

Link 2
U.S. Department of State Consent Agreements:
http://www.pmddtc.state.gov/compliance/consent_agreements.html

Link 3
Defence Security Authority's Security Responsibilities Guidance:
http://www.defence.gov.au/dmo/careers/docs/Security_Responsibilities.pdf

Link 4
ISO 27001 standard http://www.27000.org/iso-27001.htm

Link 5
Information Security Manual published by the Defence Signals Directorate:
http://www.dsd.gov.au/infosec/ism/index.htm

Annex 3: Pro Forma Technology Control Plan

Begins on next page

TECHNOLOGY CONTROL PLAN (TCP)

Replace ‘Company’ (case sensitive) with your company’s name and edit the document to suit your organisation’s needs and circumstances.

Issue Date March 2013

TABLE OF CONTENTS

1. INTRODUCTION

This Technology Control Plan (TCP) provides guidance to all Company personnel and approved contractors for the protection and handling of Controlled Technology in accordance with Technology Assistance Agreements (TAAs), Manufacturing Licence Agreements (MLAs), Warehouse Distribution Agreements (WDAs) and U.S. Export Licences to which Company is a party.

In addition, the requirements and procedures described in this plan are to be equally applied to the Controlled Technology available under Australian and other national and multinational Technology Control arrangements, regardless of the point of origin.

The TCP has the endorsement of the Managing Director of the Company and Board of Directors. The TCP is supported by a range of security instructions contained in the Export Controls Management System and associated systems, protocols and procedures.

At each location/facility where Controlled Technology is handled, an addendum to this TCP may be produced to clarify any local procedures including site specific security and trade control plans. These local procedures only supplement and do not change the requirements of this TCP.

Definitions of the various unique terms used in this document are included in the Definitions and Abbreviations paragraph (14), later in this document.

2. GENERAL POLICY

It is the policy of Company to comply with all applicable legal requirements wherever it conducts business. Company takes this obligation seriously at every level of operation and devotes substantial resources to compliance. This faithful attention to legal and regulatory compliance is aimed at preserving Company's good name nationally and abroad, preventing inadvertent breaches, and assuring operational efficiencies that are often subject to complicated regulatory controls.

Some of Company's most significant projects involve contracts and co-operation with the U.S. government and U.S. companies. These projects are invariably subject to U.S. export controls embodied in the U.S. International Traffic in Arms Regulations (ITAR) and the U.S. Export Administration Regulations (EAR).

The objective of this Technology Control Plan (TCP) is to ensure that:

a) U.S. Controlled Technology in Company's custody or control (and which is also National Security Classified Material) is protected and handled in accordance with the requirements of the Defence Industrial Security Program (DISP) and ITARs; and

b) U.S. Controlled Technology in Company's possession (which is not classified) is protected and handled in accordance with Company's contractual obligations and the requirements of U.S. Export Licences.

While most U.S. technology and technical information in Company's possession is not classified, it is nevertheless considered to be sensitive and subject to distribution limitations and restrictive markings. Such material is generally provided to Company with the explicit approval of the U.S. Government for use in a specific defence project, on the understanding that it will be protected from a change of end-use or unauthorised disclosure under the terms of the relevant contract and/or U.S. Agreement or Export License. Any defence technology that has been generated by Company from U.S.-sourced technical information must be accorded the same level of protection as the original technical information.

Company will equally respect the compliance and regulatory requirements for all Controlled Technology regardless of the point of origin.

3. APPLICABILITY

The application of regulations and corporate rules, regarding Technology Control, is incumbent upon every member of staff, permanent or temporary, and in particular those who have management responsibility and those who have import/export and /or Technology Control compliance responsibilities.

If these rules are not applied, the consequences for Company could be significant and include the loss of key commercial contracts.

While this plan focuses on ITAR obligations, the requirements must be equally applied to controlled technology and materials that are not of U.S. origin.

Controlled technologies and materials include those described as 'dual use' items by the Export Administration Regulations (EAR) issued by the U.S. Department of Commerce.

4. BACKGROUND

4.1 OUTLINE

Company has a significant number of U.S. Department of State approved Agreements and Export Licences which allows for the use of Defence Articles, Technical Data, and Defence Services under the International Traffic In Arms Regulations (ITAR).

As a company that also deals with controlled dual use technology and materials outside of the Defence Industry environment, Company will also comply with the U.S. EAR requirements.

When classified or Significant Military Equipment (SME) is involved, Company will also have completed a Non-transfer and Use Certificate (DSP-83). This certificate and similar Australian or other foreign country certificates are generically known as 'End User Certificates'.

A DSP-83 is required before the U.S. Department of State will approve a U.S. Agreement or Export Licence for the export of classified Defence Articles and Technical Data or SME. The DSP-83 stipulates that, except as specifically authorised in the U.S. Agreement or Export Licence, or separately in writing by the U.S. Department of State, Company will not re-export (or retransfer), resell or otherwise dispose of the classified equipment or SME outside of Australia or to any other person.

Details of current U.S. Agreements to which Company is a signatory are to be maintained by the Corporate Export Control Officer (CECO) in conjunction with Export Control Officers (ECO's) in each business unit location. This data will be updated on a regular basis; however each member of Company must accept responsibility for U.S. Controlled Technology and liaise with their Export Control Officer (ECO) in their business unit or support department area to keep updated on projects subject to U.S. Technology Control.

4.2 What is Controlled Technology?

The Defence Export Control Office (DECO) defines Controlled Technology as any goods listed in the Defence and Strategic Goods List. The Defence and Strategic Goods List is the document containing the complete list of items controlled for export under the *Customs Act 1901*. It can be viewed if required at the Defence Export Control Office website. This list includes U.S. ITAR and EAR items and covers:

- **Defence and related 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).

• **Dual-use goods and technologies:** those products developed to meet commercial needs, but which may be used either as military components, or in the development or production of military systems or WMD. This may include equipment; assemblies and components; test, inspection and production equipment; materials; software; and technologies.

Technologies' relates to the supply of any specific information necessary for the development, production or use of goods, such as instructions, skills, training and working knowledge that is provided in manuals, blueprints, diagrams, or through written and recorded media or devices, these 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
- Information/instructions to operate, maintain, repair, modify the item

Export controls are applicable to defence and dual-use goods including parts and components thereof and related materials, equipment and technologies transported to an external territory or nation, regardless of the state or working condition of the goods.

4.3 Control of Classified Information

Membership of the Defence Industry Security Program acknowledges Company's commitment to safeguarding classified material supplied for use on specific projects.

Details of the DISP and information governing Company's obligations for protecting and handling National Security Classified Material, are set out in the Defence Security Manual (DSM). Company shall at all times comply with the requirements of the DSM.

No National Security Classified Material, or information bearing another national security caveat, shall in any circumstances be disclosed to Unauthorised Persons, unless disclosure has been authorised in writing by the originating Government.

In the absence of such authorisation, any disclosure of National Security Classified Material to an Unauthorised Person, whether in the course of employment or otherwise, constitutes a breach of the DISP and may result in prosecution under the *Crimes Act 1914.*

Obligations on Company in Australia under this TCP are in addition to (and do not replace) any obligations of Company under the DSM. To the extent that any requirement of this TCP is inconsistent with the DSM, DSM governance prevails.

4.4 Management of U.S. Controlled Technology

Any Defence project involving U.S. persons, hardware, defence services or technology will be subject to strict licensing and compliance requirements under the ITAR. Exports of U.S. military hardware and technology invariably require a U.S. Agreement or Export License to be in place, and technology transfers involving such technology are governed strictly by the terms and conditions of U.S. Agreements and Export Licences.

Certain fundamental requirements are to be adhered to within Company in connection with projects subject to the ITAR, namely:

a) U.S. Controlled Technology is not to be used for any purpose other than authorised under the original contract and U.S. Agreement or Export Licence without the prior written approval of the U.S. Department of State.

b) Except as specifically authorised in the U.S. Agreement or Export Licence, U.S. Controlled Technology must not be transferred by any means (including by e-mail, electronic facsimile, visually or word of mouth) from Company to another Australian company or individual, or be re-exported (or retransferred) from Company to an overseas company or individual, without the prior written approval of the U.S. Department of State.

c) Australian products produced or manufactured from, or using, U.S. Controlled Technology (including technical data or defence services for that product) must not be transferred by any means (including by e-mail, electronic facsimile, visually or word of mouth) from Company to another Australian company or individual, or be re-exported (or retransferred) from Company to an overseas company or individual, without the prior written approval of the U.S. Department of State.

d) 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[1]. 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.

Similarly Company will also apply these general requirements to controlled items specified in the U.S. EAR, or similar Australian or other countries regulations.

5. ORGANISATION AND RESPONSIBILITIES

5.1 General Company Organisation

The day to day management of Company is vested in the Managing Director. The management of, and ultimate responsibility for, Company's Export Controls Management System (ECMS) is vested in the Corporate Export Control Officer (CECO). The CECO is assisted at the business unit level by the Export Control Officers (ECOs) at each business unit.

The ECO in each business unit has the responsibility for any and all National Security Classified Material and all Controlled Technology (regardless of origin) received by Company and used within that area.

Each ECO shall ensure that:

a) National Security Classified Material is administered in accordance with DISP; and

b) U.S. Controlled Technology is administered in accordance with this TCP, and any additional specific requirements that may be included in contracts or in U.S. Agreements or Export Licences.

[1] In late 2006, the Defence Department reached agreement with the US State Department that Australian dual-national employees of the Defence Department and Australian companies who have a RESTRICTED security clearance and need to know do not need to provide nationality information or Non-Disclosure Agreements
This agreement does not apply to non-citizens (e.g., exchange officers) or dual-nationals of ITAR 126.1 proscribed countries. And, in relation to company employees, it only applies to projects and programs which are intended for the ultimate end-use of the Australian Defence Department, as demonstrated by Defence being a TAA signatory or by reference to a Defence Capability Plan project

5.2 Corporate Export Control Officer

The Corporate Export Control Officer (the "CECO") reports to the General Counsel and is the Company employee responsible for maintaining details of all current U.S. Agreements (MLAs, TAAs) to which Company is a signatory.

The CECO must be an Australian citizen, an ITAR Authorised Person and ultimately responsible for Company's compliance with this TCP. The CECO and each ECO shall be identified to all Company employees within the specific Company business units.

The responsibilities and job description of the CECO are set out in detail in Attachment 1 to this TCP. This document, amongst other mandatory requirements, requires that the CECO conduct facility compliance audits as directed by the Board of Directors throughout Company in accordance with the requirements of this TCP.

5.3 Export Control Officer

The CECO shall be entitled to delegate the administration of his/her responsibilities under the above organisational responsibilities, in relation to compliance requirements to ECO at each business unit.

The ECO may be the Security Officer appointed under the DISP and will have the primary responsibility for all Import and Export requirements applicable to that specific business unit.

An export permit, or written confirmation from an Export Control Officer ("ECO") is required before Company or any employee in Company's name may export or transfer any item to another country. The ECO shall manage and administer all aspects of these requirements based on information to be provided by the relevant Business Unit or employees.

No employee, other than an ECO may apply for any import or export authorisation. Any employee wishing to export or transfer an item to another country is required to provide a full brief of information regarding the proposed export or transfer to the ECO. The ECO shall then determine whether an export permit is required and, if it is required, initiate the process to obtain one.

Generally, the ECOs shall be responsible for ensuring compliance with this TCP and applicable U.S. regulations. The particular responsibilities and job description of the ECO are at Attachment 2.

5.4 Employees and Contractors

All Company personnel and approved contractors, with access to U.S. Controlled Technology, must familiarise themselves and comply with the requirements of this document (TCP). A controlled copy of the TCP is available for viewing on the Company Intranet. All employees and contractors must sign an Acknowledgement of Receipt (Attachment 4) indicating they have been briefed on the TCP and understand their obligations.

Any breaches of the requirements outlined in this TCP will be viewed very seriously, and may lead to disciplinary action or termination of employment if appropriate.

Breaches of requirements are also subject to the provisions of the Company Code of Ethics and the associated Company Ethics policy and framework.

6. RULES AND CONTROLS GOVERNING ACCESS TO TECHNOLOGY

6.1 General Requirement

Irrespective of any individual's security or other status, that may permit access to technology and/or classified material, the general principle of a 'need to know' must be applied prior to access being granted.

6.2 Export

Under the ITAR, the disclosure of U.S. Controlled Technology in Company's possession to non authorised ITAR parties is considered to be an export.

Export controls are applicable to a wide range of Defence and related goods and technologies, including dual-use applications. Controls also include goods that are being exported for the purpose of:

a) return to manufacturer or owner

b) repair (and subsequent return to Australia)

c) demonstration or loan on a temporary basis, such as for display in trade shows

No employee may export or transfer any item to another country without an export permit or confirmation in writing from the ECO that no export permit is required.

In addition, no Technical Assistance Agreement, Manufacturing License Agreement, End User Certificate (e.g. DSP-83), or any other document containing any restriction on Company's use of Controlled Items may be executed or signed or accepted by Company without the prior approval of the General Counsel.

6.3 Information Technology – IT security

Company shall at all times comply with the requirements of Australian Security Regulations, in particular Part 4 (Information and Communications Technology Security) of the eDefence Security Manual (DSM), regarding the quarantine and control of information systems which receive or hold National Security Classified Material.

In relation to U.S. Controlled Technology, Company staff shall at all times comply with the requirements of the Company Information Systems ITAR Security Framework. This document describes the framework by which information, in electronic form, pertaining to technology protected under the ITAR will be controlled within Company. This Framework requires the implementation of information system controls to protect U.S. Controlled Technology stored on Company IT systems from access by Unauthorised Persons and that electronic communications between Company and Unauthorised Persons shall not disclose U.S. Controlled Technology.

In addition, Company staff shall comply with the Company Information Technology and Services Policy, Internet & E-mail Security Framework and the Data Security Framework.

Attention is also drawn to the Company Information Security directives requirements that are published in the Company *Securities Directives Manual*.

6.4 Access to U.S. Controlled Technology

Access to U.S. Controlled Technology in the possession of Company shall not be granted to:

a) any person in a country other than Australia or the United States; or

b) an Unauthorised Person, including any National of a country other than Australia or the United States;

Unless the prior written approval of the U.S. Department of State has been obtained.

The ECO has access to and responsibility for the maintenance of detailed records of all personnel authorised to access U.S. Controlled Technology. These records are specific to each U.S. Agreement.

6.5 U.S. Controlled Technology and U.S. Agreements

ECOs, in conjunction with the Contracts Manager, are to maintain a detailed register applicable to their specific business unit or support department of all U.S. Agreements and Export Licences, and if applicable, associated Non transfer and Use Certificates (DSP - 83).

U.S. Controlled Technology is to be stored, used and accessed at Authorised Facilities, in accordance with the following requirements:

a) the location of U.S. Controlled Technology, and all movements of this technology out of those Authorised Facilities, is to be kept in a register maintained by the ECO (Appendix A);

b) the details of persons who are approved for access to U.S. Controlled Technology are to be kept in a register maintained by the ECO (Attachment 6);

c) access to U.S. Controlled Technology shall be controlled and monitored by the ECO in accordance with the requirements of the relevant U.S. Agreement or Export Licence; and

d) physical storage requirements (as detailed in the ECMS) are to be complied with.

ECOs are to ensure that abovementioned registers, and the additional records required in accordance with the ECMS, are available to trace the receipt and dispatch of all Defence Articles and data identified as U.S. Controlled Technology.

When reviewing TAAs and MLAs ECOs must confirm with the CECO the latest agreed wording requirements.

All TAAs and MLAs, following development, or amendment, by the relevant ECO, are to be checked by the Company General Counsel and following negotiation, signed in accordance with the Company Authorities Manual.

DSP – 83's are to be signed pursuant to the Company Authorities Manual.

6.6 Physical Security

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

a) adequate locking devices for external and internal doors, windows, gates and fences;

b) security patrols and or monitoring systems to deter and detect Unauthorised Persons entering the facility; and

c) positive identification, recording, and tracking of all employees and visitors.

Company 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.

6.7 Export of Software

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

An export of ITAR-controlled software occurs when software is transferred by any means to an Unauthorised Person, whether or not the Unauthorised Person is located in Australia or overseas. For example, an export of ITAR-controlled software occurs when that software is:

a) downloaded to locations (including electronic bulletin boards, Internet file transfer protocols, and World Wide Web sites) either within Australia; or

b) transferred to an Unauthorised Person outside Australia through communications facilities accessible to Unauthorised Persons.

It is the responsibility of all Company employees who have access to ITAR-controlled software to prevent its export/re-export (or retransfer) by any means.

6.8 Export of Technical Data

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

Export, re-export or retransfer of ITAR-controlled Technical Data occurs when that data is transferred by any means to an Unauthorised Person, whether or not the Unauthorised Person is located in Australia or overseas. For example, an export, re-export or retransfer of ITAR-controlled Technical Data can occur by:

a) visual disclosure;

b) telephone discussions;

c) electronic communications;

d) facsimile communications;

e) face to face discussion, or

f) through communications facilities accessible to Unauthorised Persons.

It is the responsibility of all Company employees who have access to ITAR-controlled Technical Data to prevent its export/re-export (or retransfer) by any means, including those listed above.

7. CLASSIFICATION AND MARKING OF INFORMATION

7.1 General

The Company *Information Security Classification, Marking and Access Framework* details arrangements for:

- Identifying information according to type and format;
- Classifying information according to its sensitivity;
- Applying appropriate security markings to information, and
- Correctly handling information according to security markings

The framework includes the classification and marking requirements to be applied to any information that includes controlled technology.

Controlled Technology markings, where required, are in addition to any National Security, or other marking requirements.

7.2 Controlled Technology

Where information relates to Controlled Technology e.g. information relating to technology subject to U.S. International Traffic in Arms Regulations, and it has not already been appropriately marked, personnel are to apply relevant markings. (Illustrated in detail at annex A4 of of *Information security Classification, Marking and Access Framework).*

Where the application of relevant markings has been required, to previously unidentified Controlled Technology, appropriate feedback should be given (where known) to the originator/source.

7.3 Destination Control Statements

In addition to any security markings, Information Owners preparing paper documents that incorporate U.S. Controlled Technology information are to integrate the required non-transfer commitments by Company. 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 passed to Company or its previous entities, by Defence, and Official Information Security markings had not been applied), the following 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.)

8. HANDLING OF U.S. CONTROLLED TECHNOLOGY

> **WARNING:** Control requirements for all U.S. Controlled Technology, once identified as requiring ITAR compliance, do not diminish with the age of the technology. ITAR requirements remain in place unless identified/advised to the contrary by the U. S. Department of State.

8.1 Physical Storage Security Requirements

U.S. Controlled Technology shall:

a) be stored in areas which are designated as Authorised Facilities by each business unit ECO;

b) be stored in secure cabinets, safes, storage systems, rooms, which may be accessed by key and which cannot be moved by normal human exertion; and

   i) not be removed from an Authorised Facility without prior written approval from the relevant ECO and only in accordance with this TCP or an applicable U.S. Agreement or Export Licence; and

   ii) not be left unattended within an Authorised Facility, unless stored securely in accordance with sub-paragraph b.

8.2 Electronic Storage of U.S. Controlled Technology

U.S. Controlled Technology shall be stored only on servers which can only be accessed by "Authorised ITAR Persons" who have the right to access U.S. Controlled Technology. Access will only be granted by the ECO.

Backup copies of files/directories/servers containing U.S. Controlled Technology will be stored in secure areas which cannot be accessed by Unauthorised Persons.

Copies of files containing U.S. Controlled Technology must be controlled at all times, with complete traceability records kept.

8.3 Transfer or Transmission of U.S. Controlled Technology

Where Company is authorised to transfer U.S. Controlled Technology either within Australia, within Company, to other approved companies within Australia, or outside the Australian national boundaries to approved companies, then the following is to apply:

a) Approval for the transfer is to be obtained from the ECO (who will ensure that the ITAR Licence or Agreement relevant to the article permits the transfer of the article);

b) If the U.S. Technology is in electronic format, the data is to be transmitted by electronic transfer (i.e., by e-mail, subject to the Company Internet and E-mail Security Framework);

c) Hard copies of documents, files, etc. are to be transferred in accordance with the procedures applicable to Australian RESTRICTED/PROTECTED classified material; and

d) Equipment to be transported only by an approved carrier. (refer to http://scec.gov.au/introduction/documentrequest for SCEC endorsed couriers)

Transfer of U.S. Controlled Technology is not to occur without the approval of the ECO, who will verify that addressee/s are authorised to receive the technology.

The preferred method of transfer or transmission of U.S. Controlled Technology is by electronic communication. Any such electronic transfer or transmission may only be conducted in accordance with the Company Information Systems ITAR Security Framework. Data links between Company facilities are encrypted. To transfer electronic copies of U.S. Controlled Technology within Company, the sender is to ascertain if the addressee is authorised to access the technology. The Message Options of "Request a delivery receipt for this message" and "Request a read receipt for this message" are to be enabled to verify successful delivery. If the receipt and read receipts are not received within 24 hours, IT is to be contacted to trace the message. The receipt and read receipt are to be saved as proof of delivery.

Where the electronic transfer of U.S. Controlled Technology is to a recipient external to Company, the sender, as well as meeting the requirements detailed in the Company Internet and E-mail Security Framework, is to ascertain if the addressees are authorised to access the technology. Note that unless the addressee is authorised to receive the U.S. Technology, the prior written approval of the U.S. Department of State will be required before it is transmitted.

When sending U.S. Controlled Technology utilising encryption, the sender is to encrypt the contents with the addressee's public encryption key, and will digitally sign the message with their own (the senders) private key.

In the event that U.S. Controlled Technology cannot be communicated securely by electronic transmission in accordance with the above Framework, the relevant U.S. Controlled Technology may only be transferred by way of registered courier services provided by an approved courier company, or locked brief case carried by an authorised Company employee (ensuring that the brief case remains in the presence of the employee at all times until delivery).

8.4 Destruction of U.S. Controlled Technology

U.S. Controlled Technology may only be destroyed if the originator of the technology has consented to the destruction via a TAA, MLA or Licence. Where the originator is unknown, or is unable to be contacted, a copy of the Destruction Certificate is to be kept for a minimum of 5 years.

U.S. Controlled Technology stored in electronic form, physical hard copy, removable media or stores shall be destroyed by two appropriately authorised staff and with written approval of the ECO in the following manner:

a) Electronic form – erasure from the U.S. Controlled Technology store;

b) Physical hard copy – shredded in a classified document shredder and the waste placed into a classified waste bin;

c) Removable media – physically destroy the media and any magnetic components thereof, the waste shall be placed into a classified waste bin;

d) Physical materials/equipment are to be destroyed in an appropriate manner, and

e) Record of destruction (Destruction Certificate) signed and witnessed by the staff members performing the destruction to be completed.

After destruction and a Destruction Certificate have been completed; the item is to be deleted from the ERP system. A copy of the Destruction Certificate is to be kept for a minimum of 5 years.

9. CONTROL OF VISITING UNAUTHORISED PERSONS

9.1 Visitor Register

Each Company facility shall ensure that all visitors sign the relevant visitor register prior to entry into an Authorised Facility. It is the responsibility of the Company host to establish whether a visitor represents an Unauthorised Person, and to provide an appropriate escort.

9.2 Visitor Escort Requirements

Unauthorised Persons visiting Company Facilities are to be escorted at all times by Company employees and shall wear unique identification cards at all times. This unique visitor's identification card is to be easily identifiable.

Access to facilities cleared to store National Security Classified Material shall be in accordance with the DISP and local Company procedures.

Access to Authorised Facilities shall not be granted to Unauthorised Persons, except in accordance with this TCP.

Company escorts must be familiar with the restrictions on access to relevant U.S. Controlled Technology. It shall be the responsibility of the Company escort personnel to ensure that visitors issued with unique visitors badges do not have access to U.S. Controlled Technology unless access is permitted under relevant U.S. Agreements or Export Licences or exemption, and then only when approved by the ECO.

9.3 Employee Responsibilities

The ECO is to ensure that all relevant Company personnel in an area containing U.S. Controlled Technology are warned in advance of a visit by any Unauthorised Person, and are aware of:

a) the U.S. Controlled Technology, if any, licensed for disclosure;

b) the requirements and limitations imposed by the relevant U.S. Agreement, and any applicable provisos;

c) the areas and activities of the Facilities to which the visitor will be given access; and

d) visitor escort requirements and other requirements of this TCP.

Any breaches of the requirements outlined in this TCP will be viewed very seriously, and may lead to disciplinary action or termination of employment if appropriate.

Breaches of requirements are also subject to the provisions of the Company Code of Ethics and the associated Company Ethics policy and framework.

10. RECRUITMENT AND EMPLOYMENT

10.1 Recruitment Policy

Company Company's Recruitment and Selection Policy (AUS/00369), Framework (AUS/00953) and Personnel Request Form (HR-ADI-FM-007) ensure that external and internal recruitment tasks address the following issues:

a) In relation to each position for which a recruitment process is to be tasked (whether internally or externally), an assessment is to be made as to whether the person employed in the position will require access to National Security Classified Material and/or U.S. Controlled Technology in the ordinary course of his/her duties;

b) If such access is required, it shall be a requirement of the job description that the prospective employee be capable of fulfilling the security and other requirements of access to the relevant material;

c) If an Unauthorised Person is the most qualified candidate and is proposed to be employed, it shall be a condition of employment that the relevant approvals are obtained from relevant U.S. authorities prior to granting the employee such access; and

d) Prior to recruitment of any such person, appropriate nationality data shall be obtained by Company to ensure that Company does not inadvertently breach any obligation under the DISP or any U.S. Agreement or Export Licence.

10.2 Authorised Persons Induction

This TCP is to be made available to all authorised Persons, who are to be informed of their responsibility to treat all technical information obtained during their employment at Company on a company proprietary basis. A controlled copy of the TCP is available for viewing on the Company Intranet.

10.3 Employment of Unauthorised Persons

Unauthorised Persons shall only be employed on the authority of the HR Vice President, and then only in areas where U.S. Controlled Technology is **not** used. If an Unauthorised Person is employed, that person shall not be involved in any work that involves the disclosure of U.S. Controlled Technology unless the U.S. Government has authorised access in the context of amendment to a U.S. Agreement or Export Licence, or separately in writing.

10.4 Unauthorised Persons Induction

This TCP is to be made available to all Unauthorised Persons, who are to be informed of their responsibility to treat all technical information obtained during their employment at Company on a company proprietary basis. Unauthorised Persons are also to be made aware of their responsibility for compliance with this TCP and related Company policies and procedures, especially in regard to no access to U.S. Controlled Technology.

10.5 Non-Disclosure Statement

All employees of Company who are nationals of a country other than Australia or the U.S. and who are authorised under an appropriate U.S. Agreement or Export Licence to access U.S. Controlled Technology, and who have access to U.S. Controlled Technology shall be required, upon commencement and termination of his/her employment with Company, to sign a Non-Disclosure Statement (Attachment 7). This statement shall certify that they will not and/or have not given or disclosed to any Unauthorised Person any U.S. Controlled Technology.

Requirements for Non-Disclosure Statements can vary between various TAA and MLA, and should be confirmed with the relevant ECO prior to either providing access, or requiring the completion of a Non-Disclosure Statement.

10.6 Temporary Staff/Subcontractors

All individual temporary/labour hire staff, for the purposes of Controlled Technology access, shall be treated as a Company Employee, and the procedures in this TCP shall apply to them.

Subcontracts for contract labour, subcontracted supplies or work to be performed by Company subcontractors within Australia and who require access to U.S. Controlled Technology, shall be included (where appropriate as a sub-licensee) in the relevant U.S. Agreement.

Exceptions to this policy can only be made if the appropriate U.S. Agreement or other license clearly authorises the exception.

11. TRAINING

11.1 Authorised Employees

All employees of Company who are authorised to access either National Security Classified Material or U.S. Controlled Technology shall attend a compulsory comprehensive training briefing provided by the ECO. This briefing is to be conducted before access to National Security Classified Material and/or U.S. Controlled Technology is undertaken by that employee/contractor in that particular area of Company. The training will cover:

a) Importance of safeguarding Classified and Controlled articles and data held within the company;

b) The role of the company and the employee under the DISP (Defence Industrial Security Program) and other Australian Security Regulations applicable to the company;

c) The obligations and responsibilities of the company and the employee under the DISP (National Security Classified Material);

d) The roles and responsibilities of security cleared employees;

e) A detailed review of the relevant U.S. regulations governing the company's activities;

f) The nature of the company's obligations for U.S. Controlled Technology and the terms of the U.S. Agreements to which the company is a party;

g) Procedures for obtaining U.S. Government approvals and when those approvals are required; and

h) The prohibition on Unauthorised Persons accessing Classified and U.S. Controlled Technology.

11.2 Unauthorised Employees/Subcontractors

All Unauthorised Persons employed by Company will be:

a) informed that they will not be entitled to access any National Security Classified Material unless written approval of the Australian government in received in accordance with the DISP;

b) informed that prior written U.S. Government approval will be required before they may have access to the relevant U.S. Controlled Technology, unless access has already been approved under a U.S. Agreement or Export Licence. Further, Third Party Foreign Persons/Dual Citizens who are authorised to access U.S. Controlled Technology will be informed as to their responsibility to treat all U.S. Controlled Technology obtained during their employment in accordance with this TCP;

c) made responsible and liable for adherence to facility security rules, policies and procedures relating to security and U.S. Controlled Technology;

d) briefed in those areas of export control and export licensing which are pertinent to their activities; and

e) notified of the sanctions and penalties that could be imposed on the U.S. exporter and Company for any deliberate violation of security and U.S. Controlled Technology regulations.

11.3 Export Control Officers

ECOs shall complete an additional advanced training program with regard to the requirements of U.S. export restrictions. In particular, in relation to:

a) An in depth understanding of the relevant Australian legislation and U.S. regulations;

b) The nature of the Company's obligations for U.S. Controlled Technology and the terms of the U.S. Agreements to which the company is a party;

c) Procedures for obtaining U.S. Government approvals and when those approvals are required; and

d) The prohibition on Unauthorised Persons accessing National Security Classified Material and U.S. Controlled Technology.

11.4 Annual Refresher Training

In addition to the completion of Security Induction Training prior to commencement of work with Company, all employees of Company will undergo annual refresher training programs, to ensure they are familiar with all Australian Security Regulations and U.S. Regulations applicable to Company.

The CECO and all ECOs will undergo annual refresher training to reiterate the contents of this TCP, their responsibilities and provide them an update on any additions/changes to the ITAR.

12. MAINTENANCE OF RECORDS

Records of Company export and re-export (or retransfer) of U.S. Controlled Technology and associated documentation shall be maintained for a minimum of five (5) years from the date of shipment or transfer, or the expiration of the applicable U.S. Agreement or Export Licence, whichever is longer, including:

a) Copies of U.S. Agreements or other licences, amendments, attachments, riders, conditions and provisos;

b) Supporting documentation such as import certificates, Nontransfer and Use Certificates, etc;

c) Register of U.S. Controlled Technology received;

d) Register of shipments or transfers of U.S. Controlled Technology authorised by U.S. Agreement or other licence or exemption;

e) A record of electronic communications to/from employees who have access to U.S. Controlled Technology; and

f) A record of all visitors accessing Company Authorised Facilities.

Note that a five (5) year retention requirement is the minimum ITAR requirement. Reference should also be made to other Company and/or Project specific procedures and requirements, on records and archiving, which may require extended retention periods.

Refer also to Attachment 3 and Appendix A of this TCP further details on record requirements and a sample register. Similar records should also be maintained and retained for the Controlled Technologies of other countries that have been entrusted to Company.

13. APPLICABLE DOCUMENTS

This plan/procedure requires reference to the following documents: Examples Only)

a) Company Security Policy

b) Information Systems ITAR Security Framework

c) e-Defence Security Manual

d) Local Security Standing Orders (SSO)

e) Company Information Technology and Services Policy

f) Company Internet & Email Security Framework

g) Company IT Security Operations Framework

h) Company Information Security Classification, Marking and Access Framework

i) Company Security Officer (CSO) Duty Manual

j) Company Authorities Manual

k) Company Securities Directives

14. DEFINITIONS AND ABBREVIATIONS

Within this document, the following terms shall have the following meanings:

"Company" or "the company" means Company Pty Limited or its successors and every Subsidiary of Company, trading as Company.

Company Defence Contract" means a contract for the supply of defence related equipment by Company.

"Authorised Facility" means a Company Facility that has been authorised by the National Export Control Officer in accordance with this TCP to receive, store and access U.S. Controlled Technology.

"Chief Information Officer (CIO)" is the Company employee responsible nationally to ensure that all Company business and support elements comply with the National Security Classified Information Systems requirements under Australian Security Regulations, the Company Information Technology and Services Policy, Internet & E-mail Security Framework and the Data Security Framework and other such functions.

"Classified Material" means material subject to the relevant national security regulation of any national government.

"Controlled Technology" refer to para 4.2 of this document.

"Corporate Export Control Officer (CECO)" is the Company employee responsible for maintaining details of all current U.S. Agreements to which Company is a signatory. Includes similar export agreements with other countries.

The CECO is also responsible to ensure that all Company business and support elements comply with the requirements laid out in this TCP. To assist the CECO, ECOs may be appointed to support individual business units in their TCP compliance obligations.

"Defence Article" has the meaning given to that term in the ITAR, and includes articles listed on the United States Munitions List (USML). A defence article is specifically designed, developed, configured, or modified for a military application. The term includes Technical Data recorded or stored in any physical form, models, mocks-ups or other items that reveal information relating to items designated on the USML.

"Defence Services" has the meaning given to that term in the ITAR, and includes:

a) the furnishing of assistance (including training), 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 Defence articles;

b) the furnishing of any Technical Data controlled by the ITAR, whether in the United States or abroad; or

c) the provision of military training in the United States or abroad, including by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

"DDTC" means the Directorate of Defence trade Controls in the United States Department of State which is responsible for administering the ITAR.

"Dual Use", In general, the term dual use serves to distinguish EAR-controlled items that can be used both in military and other strategic uses and in civil applications from those that are weapons and military related use or design and subject to the controls of the Department of

State or subject to the nuclear related controls of the Department of Energy or the Nuclear Regulatory Commission.

"Export Administration Regulations (EAR)", the EAR are issued by the United States Department of Commerce, Bureau of Industry and Security (BIS) under laws relating to the control of certain exports, reexports, and activities. They include regulations relating to "dual use" controlled items.

"Export Control Officer" (ECO)"means a Company employee appointed to ensure that all Company Import/Export business activities (normally on a regional basis) are in accordance with the requirements. It also means the employee responsible for ensuring that all requirements of this TCP are complied with in regards US Controlled Technology.

"Security Officer (SO)" means a Company employee appointed to ensure that all Company business activities in an Accredited Facility comply with the security requirements of the DISP with regards to National Security Classified Material.

"International Traffic in Arms Regulations (ITAR)" means the U.S. regulations that control the export of Technical Data, Defence articles, and Defence services specified on the USML. The ITAR is administered by the Office of Defense Trade Controls ("DTC") in the Department of State.

"Manufacturing License Agreement (MLA)" means an agreement whereby a U.S. person grants a non-U.S. person authorisation to manufacture Defence articles abroad, approved by the U.S. Government under the ITAR.

"Security Officer" is the Company employee responsible nationally for ensuring that Company business and support elements comply with Australian Security Regulations required under the Defence Industrial Security Program (DISP).

"Significant Military Equipment (SME)" means articles that are specifically identified in the USML, and which have the capacity for substantial military utility or capability thus warranting the application of special export controls by the U.S. Government (e.g., the requirement for DSP-83s).

"Technical Assistance Agreement (TAA)" means an agreement whereby a U.S. person performs Defence services for and/or discloses Technical Data to a non-U.S. person, approved by the U.S. Government under the ITAR. Assembly of Defence articles is included in this definition, provided production rights or manufacturing know-how are not conveyed (should such rights be transferred, a Manufacturing License Agreement is required).

"Unauthorised Person" means in relation to U.S. Controlled Technology, any person not authorised for access under a U.S. Agreement or Export Licence, and who has not been subsequently approved for access by the U.S. Government.

"U.S. Agreement" means any TAA or MLA or other approval in writing under relevant U.S. regulations for use and/or disclosure of U.S. Controlled Technology by Company.

"U.S. Controlled Technology" means Defence Articles, Technical Data and Defence Services exported to Company, with U.S. Government approval under the ITAR, for use by Company in relation to a Company Defence contract and identified as such to Company.

"U.S. Export Licence (or License)" means a document bearing the word "license" issued by the Director, Office of the Defense Trade Controls or his authorised designee which permits the export of a specific defence article from the U.S.

"United States Munitions List (USML)" means a listing of articles, services and related Technical Data which are designated as Defence articles and Defence services. Exports of items on the USML are controlled under the ITAR. An extract of articles listed in the USML may be found in the International Traffic in Arms Regulations (ITAR), 22 CRF 120 – 130, Part 121.

15. INFORMATION ABOUT THIS DOCUMENT

15.1 Document Management and Control

CREATION	NAME	BUSINESS GROUP / DEPARTMENT	DATE
AUTHOR	Jane Smith	ITAR Consultant	06/03/2006
REVIEWED	John Doe	Technology Control Officer	09/06/2006
REVIEWED	Jim Doe	Chief Security Officer	13/03/2006
REVIEWED	Tom Doe	Chief Information Security Officer	31/10/2006
REVISED	Mary Doe	Assist. Technology Control Manager	27/08/2007
REVISED (rev5)	Jim Doe	Chief Security Officer	30/11/2009
REVISED (rev 6)	Harry Doe	Corporate Export Control Officer	09/01/13

ISSUE	DATE	DESCRIPTION OF CHANGE	APPROVED
1.0	15/6/2006	Approved for Issue	Harry Doe
2.0	09/6/2006	Section 1 added, subsequent sections revised and renumbered, previous section 11 removed	Jane Smith
3.0	13/03/06	Revised, in line with organisational and title changes	Jim Doe
3.1	31/10/06	Revised to reflect Import Export policy and framework documents.	Jim Doe
4.0	27/08/07	Revised to include advice on U.S. State Department advice on Australian Dual Nationals.	Harry Doe
5.0	30/11/09	Reflects latest changes to ITAR's, organisational and title changes and U.S. State Department advice on Australian Dual Nationals.	Harry Doe
6.0	09/01/13	Reflects transfer the TCO duties to the ECO. Restructure of positions have also been reflected in the Position Descriptions.	Harry Doe

15.2 Enquiries

Please direct any query or suggestion regarding this document to the Corporate Export Control Officer.

Company Intranet contains a number of links to various informative Controlled Technology web sites that may be consulted for general information about export controls.

ATTACHMENT 1

POSITION DESCRIPTION – CORPORATE EXPORT CONTROL OFFICER (CECO)

Direct Reporting to: General Counsel

Location: Company, Sydney

Principal Responsibility:

To ensure compliance of Company and its employees with the protection requirements of Australian and overseas export regulations applicable to Company, including the United States International Traffic in Arms Regulations (ITAR) and specific protection requirements contained in all export/import licences issued to Company.

Secondary Responsibility:

To ensure that there are access control policies and procedures in place so that all receipts, storage, access, handling and transmission of export controlled technology or data is conducted in accordance with Company's responsibilities under relevant permits or licences and in accordance with the Company Technology Control Plan ("TCP").

Position Responsibilities:

Export and Import Controls Generally:

- Ensure that all business units and the Company strictly comply with the regulations applicable to the (re)export of controlled items.
- Liaise with supervisory authorities and professional organisations on regulatory matters.
- Responsible nationally for maintaining details of all current U.S. Agreements (MLAs, TAAs) to which Company is a signatory.
- Maintains details of any Import/ Export Control agreements with the Australian Government or other foreign countries.
- Co-ordinate and, if necessary, forward license applications, to the national authorities (this responsibility could be delegated to the Company/Units' ECO).
- Provide its expertise to support the sale & marketing activities.
- Support internal audit, outside consultants and he general counsel, in the evaluation of operational units and implementation of corrective actions.
- Monitoring and ensuring compliance with the technology security obligations for all export and import access control requirements under Australian law.
- Preparing and conducting (or coordinating) implementation plans for all matters relating to export/import security technology security compliance.
- Preparing and conducting (or coordinating) corrective action plans in relation to any identified breach of Company technology security obligations.
- Act as the General Counsel's main adviser on export compliance matters.

- Provide input to the Managing Director for the selection of the sales and industrial strategy (partnerships, technology transfer, direct offsets, etc) so that products developed and marketed are exportable under the regulations in force.
- Inform the General Counsel of any suspected non-compliance with applicable regulations, and manage implementation of corrective actions.
- Identify non-compliances and manage the implementation of corrective actions.
- Set up procedures and organisation to comply with all applicable laws and regulations, and supervise their implementation, by the relevant operational & functional departments
- Responsible for ensuring that all receipts, storage, access, handling and transmission of export controlled technology or data is conducted in accordance with Company rights under relevant permits or licences and in accordance with the Company Technology Control Plan ("TCP").

ITAR Controls:

- Responsible for ensuring compliance of Company and its employees with applicable Australian and overseas export regulations, including the United States International Traffic in Arms Regulations (ITAR) and all export/import licences issued to Company.
- Assessing project teams and processes to determine whether the technology security arrangements for the relevant TAA/MLA or other approvals (collectively the "TAA") are adequate for the project purposes.
- Advising management, in consultation with General Counsel, as to project security requirements under the TAA.
- Ensuring that project members fully understand their access and transfer control obligations under ITAR with respect to a project and the TAA.
- Conducting audits of technology security compliance of projects against the TCP and the TAA.
- Monitoring and (if necessary) correcting inadvertent "deemed export" of controlled technology to unauthorised persons/employees.

Security Procedures:

- Assist the General Counsel to develop technology security procedures (including addendums to the Company Technology Control Plan, IT security principles and physical access requirements specific to the project/area) that will ensure Company's compliance with its Australian and international obligations.

Information Technology Issues:

- Determining, in conjunction with management, employee access rights to project IT systems, and ensuring they are implemented at the project level.
- Informing and consulting with the CIO and General Counsel in relation to specific IT security requirements for projects/areas.

Training:

- Coordinate and conduct training programs for all operational employees in the project to improve technology security awareness of export and import issues (including ITAR) applicable to the project.

- Conducting training courses at the project level on “deemed exports” so that all employees are aware of the meaning of this term and the associated pitfalls.
- Conducting or support other training programs, and briefing employees and Unauthorised Persons (as referred to in the TCP), as required by the TCP.
- Provide awareness communication and training.

Maintenance of Records:

- Ensuring that required access and transfer records are maintained by Company so as to comply with the requirements of the TCP.
- Responsible for ensuring that all receipts, storage, access, handling and transmission of export controlled technology or data is conducted in accordance with Company rights under relevant permits or licences and in accordance with the Company Technology Control Plan (“TCP”).

Reporting:

- Regular informal reporting to the General Counsel, in relation to Export Control issues.
- Immediate reporting to the General Counsel of any breach or suspected breach of Company obligations in relation to export/import permits and licences.

Preferred Skills, Experience and Attributes:

- Good working knowledge of export/import requirements in Australia.
- Good knowledge of ITAR and Classified Information (DISP) would be an advantage (but training can be provided).
- Excellent communication skills with an ability to work with and get along with a wide variety of personnel and third parties.
- Ability to get the job done and work in a team.
- Excellent organisational skills and ability to prioritise.
- Accuracy and attention to detail.
- Ability to work under pressure with tight deadlines.
- Proactive attitude.
- Engineering or project management background preferred.

ATTACHMENT 2

POSITION DESCRIPTION –EXPORT CONTROL OFFICER (ECO)

Direct Reporting to: Corporate Export Control Officer

Location: Business Units throughout Australia

Principal Responsibility:

To support the CECO with ensuring compliance of Company and its employees with the protection requirements of Australian and overseas export regulations applicable to Company, including the United States International Traffic in Arms Regulations (ITAR) and specific protection requirements contained in all export/import licences issued to Company.

Secondary Responsibility:

To support the CECO ensure that there are access control policies and procedures in place so that all receipts, storage, access, handling and transmission of export controlled technology or data is conducted in accordance with Company's responsibilities under relevant permits or licences and in accordance with the Company Technology Control Plan ("TCP") and policies and frameworks and procedures referred to in it.

Position Responsibilities:

Generally support the CECO with:

- Monitoring and ensuring compliance with the technology security obligations for all export and import access control requirements under Australian law.
- Seeking advice from CECO as to any technology security access control requirements for export or import permits required for the project.
- Preparing and conducting (or coordinating) implementation plans for all matters relating to export/import security technology security compliance.
- Assist the CECO in preparing and conducting (or coordinating) corrective action plans in relation to any identified breach of Company technology security obligations.
- Ensure that the Operational Unit complies with applicable national and international import and export control laws and regulations, and act as the main interface, on import and export control matters, between internal and external stakeholders.
- Monitoring and ensuring compliance with the obligations of the Unit for all import and export control requirements under foreign and national law.
- Act as an interface, on import and export control matters, between all internal and external stakeholders
- Seek advice from CECO as to any requirements for import and export permits required for the project.
- Set up procedures and organisation to comply with all applicable import and export control laws and regulations, and supervise their implementation, by the relevant operational & functional departments;
- Co-ordinate and process all applications for import and export licences, and ensure that compliance to the terms and conditions of the approved licences are enforced.
- Manage the system for archiving documents and registers relating to import and export control.
- Follow up and improve the implementation of internal procedures.

- Develop positive relationships with regulatory authorities.
- Inform the CECO of any suspected non-compliance with applicable regulations, and manage implementation of corrective actions, with the support as required of the CECO.
- Provide input to the CECO for the selection of the sales and industrial strategy (partnerships, technology transfer, direct offsets, etc) of the Operational Unit, so that products developed and marketed are exportable under the regulations in force.
- Determining in accordance with management employee access rights to project IT systems, and ensuring they are implemented at the project level.
- Immediate reporting to the CECO of any breach of Company obligations in relation to import or export permits and licences.

ITAR Controls:

- Support the CECO in assessing project teams and processes to determine whether the technology security arrangements for the relevant TAA/MLA or other approvals (collectively the "TAA") are adequate for the project purposes.
- In the absence of the CECO, advising management, in consultation with General Counsel, as to project security requirements under TAAs.
- Support, or as required, conduct audits of technology security compliance of projects against the TCP and the TAA.
- Assessing project teams to determine whether a relevant TAA/MLA or other approval (collectively the "TAA") is adequate for the project purposes.
- Preparing draft amendments to TAAs as required.
- Ensuring that project members fully understand their obligations under ITAR with respect to a project and the TAA.
- Monitoring and (if necessary) correcting inadvertent "deemed export" of controlled technology to unauthorised persons/employees.

Security Procedures:

- Support the development of technology security procedures (including addendums to the Company Technology Control Plan, IT security principles and physical access requirements specific to the project/area) that will ensure Company's compliance with its Australian and international obligations.

Information Technology Issues:

- In the absence of the CECO, determining, in conjunction with the General Counsel and management, employee access rights to project IT systems, and ensuring they are implemented at the project level.
- Informing and consulting with the CIO in relation to specific IT requirements for the project.

Training:

On a needs basis, generally support the CECO to:

- Conduct training programs for all operational employees in the project to improve technology security awareness of export and import issues (including ITAR) applicable to the project.
- Conduct training courses at the project level on "deemed exports" so that all employees are aware of the meaning of this term and the associated pitfalls.

- Conduct or support other training programs, and briefing employees and Unauthorised Persons (as referred to in the TCP), as required by the TCP.

Maintenance of Records:

- Support the CECO in ensuring that required access and transfer records are maintained by Company so as to comply with the requirements of the TCP.

Reporting:

- Regular informal reporting CECO in relation to Technology Security issues.
- Formal written reports every 6 months to the CECO as to the status of export/import compliance by the project.
- Immediate reporting to the CECO and General Counsel of any breach or suspected breach of Company obligations in relation to export/import permits and licences.

Preferred Skills, Experience and Attributes:

- Good working knowledge of export/import requirements in Australia.
- Good knowledge of ITAR and Classified Information (DISP) would be an advantage (but training can be provided).
- Excellent communication skills with an ability to work with and get along with a wide variety of personnel and third parties.
- Ability to get the job done and work in a team.
- Excellent organisational skills and ability to prioritise.
- Accuracy and attention to detail.
- Ability to work under pressure with tight deadlines.
- Proactive attitude.
- Engineering or project management background preferred.

ATTACHMENT 3

MANAGEMENT OF U.S. CONTROLLED TECHNOLOGY AND U.S. AGREEMENTS

General

To meet the requirements of this TCP, the following actions are to be taken with regard to the receipt and handling of ITAR material.

Receipt, Storage, Dispatch or Destruction Records

The location and all movements of U.S. Controlled Technology held by Company, and movement out of the facility is to be kept in an appropriate register. Projects are to keep separate ITAR registers that record, as a minimum:

a) Unique and increasing serial number,

b) Date of Entry,

c) Type of Document,

d) Sender or Originator,

e) Reference Number,

f) Total number received or produced, and

g) Final Disposal. (Destroyed or returned).

An example of an ITAR Controlled Information Register is at Appendix A. This may be used for the record of holdings and disposal of this information.

Acknowledgement of Receipt

A formal acknowledgement of receipt should be completed upon:

a) An employee receiving a TCP briefing (Attachment 4)

b) An employee receiving ITAR controlled material (Attachment 5)

Other Records to be Maintained

A list of personnel authorised to access ITAR material is to be maintained by the ECO (Attachment 6)

Employees are required to sign a non-disclosure statement to acknowledge they understand their obligations. (Attachment 7) The ECO will maintain all NDAs.

ATTACHMENT 4

TCP BRIEFING ACKNOWLEDGEMENT FORM

Thales Technology Control Plan (TCP) Version [ ] dated [ ]

for

[*insert project/product description*]
(the Programme)

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

ATTACHMENT 5

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 Officer.

ATTACHMENT 6

LIST OF AUTHORISED ITAR PROJECT PERSONNEL FORM

Project:

TAA/MLA Ref:

Names of Personnel Authorised for Access to/Use of ITAR Material

Name	Department/Location

ATTACHMENT 7

NON-DISCLOSURE STATEMENT

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, U.S. Department of State.

_____
Print name

_____
Signature

_____
Date

APPENDIX A

1. ITAR U.S. CONTROLLED INFORMATION/MATERIAL REGISTER

1.1 Requirements

The Controlled Information/Material Register (CI/MR) is to contain a complete record of the holdings and disposal of all ITAR Controlled Technology material. The CI/MR shall be maintained by the ECO. Separate CI/MR's may be maintained where practical.

The nominated ECO is to be responsible for the compilation and maintenance of the register; the ECO is to be responsible for supervising the register.

All entries are to be made in blue or black ink, or black or blue ball point pen, with closure of a serial to be struck through in red pen or ball point and:

a) The Serial Number of the entry is to be entered in column (a), and is to be consecutive. This number is to be entered on each document before filing to assist with identification.

b) The date of entry is to be entered in column (b).

c) The type of document/material is to be entered in column (b), e.g. D _ drawing, F _ soft copy file, etc..

d) The details of the originator are to be entered in column (d).

e) The reference or file name is to be entered in column (e). Where there are multiple files on the media (e.g., CD) then a print out of the files may be filed with to the CI/MR.

f) The date of origin is to be entered in column (f).

g) The subject or title is to be entered in column (g).

h) The total number received is to be entered in column (h).

i) Disposal details are to be entered in column (i) and (j) to record details of transfer or destruction. Remarks in column (k) are to record additional information, including destruction method. Where the files are soft copy files, then the details of deletion from the server must also be included. Two members are to witness the destruction, and their names entered in the CI/MR.

The CI/MR is to be retained for a minimum of Five (5) years after the last entry is made, or as required by any specific contract requirements.

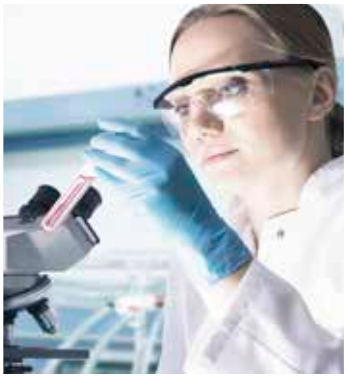
1.2 REGISTER (example)

FOLIO NO _____…

RECEIPT DETAILS								DISPOSAL DETAILS		
Serial No.	**Date of Entry**	**Type of Document**	**Sender or Originator**	**Reference No.**	**Date of Origin**	**Title or Subject**	**Total No. Received or Produced**	**FINAL DISPOSAL**		**REMARKS**
								Despatched To or Enclosed In (*Ref no. of file and folio no.)*	**Receipt Serial No. and Date Returned**	*(To include destruction particulars when applicable or signature of recipient if receipt form is not used)*
(a)	**(b)**	**©**	**(d)**	**(e)**	**(f)**	**(g)**	**(h)**	**(i)**	**(j)**	**(k)**







METROPOLITAN OFFICES

SYDNEY
51 Walker Street
North Sydney NSW 2060
PO Box 289
North Sydney NSW 2059
Tel: 02 9466 5566
Fax: 02 9466 5599

MELBOURNE
20 Queens Road
Melbourne VIC 3004
PO Box 7622
Melbourne VIC 8004
Tel: 03 9867 0111
Fax: 03 9867 0199

BRISBANE
202 Boundary Street
Spring Hill QLD 4004
PO Box 128
Spring Hill QLD 4004
Tel: 07 3244 1777
Fax: 07 3244 1799

CANBERRA
L2, 44 Sydney Avenue
Forrest ACT 2603
PO Box 4986
Kingston ACT 2604
Tel: 02 6233 0700
Fax: 02 6233 0799

ADELAIDE
L1, 45 Greenhill Road
Wayville SA 5034
Tel: 08 8394 0000
Fax: 08 8394 0099

REGIONAL OFFICES

ALBURY/WODONGA
560 David Street
Albury NSW 2640
PO Box 1183
Albury NSW 2640
Tel: 02 6041 0600
Fax: 02 6021 5117

BALLARAT
L1, 1021 Sturt Street
Ballarat VIC 3350
PO Box 640
Ballarat VIC 3353
Tel: 03 5331 7688
Fax: 03 5332 3858

BENDIGO
87 Wills Street
Bendigo VIC 3550
Tel: 03 5440 3900
Fax: 03 5443 9785

NEWCASTLE
Suite 1, "Nautilos"
265 Wharf Road
Newcastle NSW 2300
PO Box 811
Newcastle NSW 2300
Tel: 02 4925 8300
Fax: 02 4929 3429

WOLLONGONG
L1, 166 Keira Street
Wollongong NSW 2500
PO Box 891
Wollongong East
NSW 2520
Tel: 02 4228 7266
Fax: 02 4228 1898

AFFILIATE

PERTH
Chamber of Commerce & Industry
Western Australia
180 Hay Street
East Perth WA 6004
PO Box 6209
East Perth WA 6892
Tel: 08 9365 7555
Fax: 08 9365 7550

BIZassistInfoline
@aigroup®

For all your workplace related questions,
please call 1300 78 38 44

AIG13051