Export Controls Awareness Training
For SPO Staff

Your Presenter – Eva Galfi

About Eva Galfi

- Sydney-based consultant on U.S. and Australian Export Controls
- Principal, International Trade Advisors
- Certified ITAR Professional (CIP)
- Certified U.S. Export Compliance Officer (CUSECO)
- Masters in International Management, Trade emphasis
- 20 years experience in consulting, U.S. and Australia
- Editor, Australian Best Practices Guide for the Management of Controlled Exports and Technology
Goals of the Training

You will learn:

- What Export Controls are
- Why US export controls are important in Australia
- What happens when you violate export controls
- Permissions for accessing and moving export-controlled technology
- About the FMS program, MoUs and LoAs
- How export controls limit access to controlled technology at the SPO
- Receipt and marking of export-controlled technology
- Transferring/Retransferring of export-controlled technology
- Storage and destruction of export-controlled technology
- Record keeping for export-controlled technology
- Keys to effective compliance with export controls
Overview of Export Controls

◆ What they are:
  ○ Export Controls are regulations, overseen by government agencies, put in place to protect national security, promote foreign policy, and in some cases to control short supplies.
  ○ The U.S., Australia, Japan, the UK, France and many other countries also maintain lists of technology controlled for export, however the U.S. is the only country that controls these assets extra-territorially for the lifecycle of the technology.
  ○ The two key U.S. Regulations governing U.S. origin “Export Controlled Technology” are the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR).
  ○ The term “export” can have different meanings depending on how it is defined by a particular piece of legislation.
  ○ Where government approval is not obtained prior to “Export”, this constitutes a violation that can lead to financial and reputational consequences.
  ○ Hardware, software, and technical data are all subject to export controls.

Compliance with Export Controls

◆ Why are they important for industry:
  ○ Tendering opportunities
  ○ Compliance with current contractual terms
  ○ Avoid fines, penalties and reputational damage

◆ Why are they important to DoD:
  ○ AU is a party to international arrangements and agreement (Waasenaar, Australia Group, Etc)
  ○ We need to remain a safe pair of hands to continue to access US technology and thereby safeguard our own defence capability

◆ What needs to be done to ensure compliance?
  ○ Documenting policies and procedures
  ○ Respecting access controls
  ○ Marking and storage protocols
  ○ Verifying approvals are in place before transaction (export, re-export, transfer, re-transfer, upload, email, destruction, etc.)
  ○ Keeping accurate and consistent records
What is an “export”?

**Under the ITAR**
- Includes tangible (something you put in a box) or intangible (an email or video chat)
- Not necessarily cross-border, can be sent to another SPO, industry partner or other legal entity in Australia

**Under the EAR**
- Includes tangible or intangible exports
- Not necessarily cross-border, can be sent to another SPO, industry partner or other legal entity in Australia

**Under Australian Legislation**
- Must be cross-border (e.g. from a place in Australia to a place outside of Australia)
- Can be tangible or intangible

*An Approval must be in place prior to ‘export’, otherwise it is a violation of these export controls*
Export Approval Types

ITAR Licenses

ITAR Agreements
- TAA
- MLA

Licenses and Permits (EAR and AU)

License Exceptions (EAR)

Exemptions (ITAR)

Defence Trade Cooperation Treaty (ITAR exemption)

Third Party Retransfer (ITAR and EAR procured under FMS)

General Correspondence (ITAR)

Access to Export Controlled Technology

You must have an approval to get or give access.

The approval must describe the technology you are working with.

The approval must cover the scope of work you are engaged in.

The approval must be current (not expired) unless it relates to data.

You must be an Authorised Person as determined by your SPO’s Export Control Officer.

Access by Unauthorised Persons is a violation, even where they work for your organisation. Not all SPO staff are authorised to access export controlled technology.

The list of Authorised Persons is project / technology specific. Lists of Authorised Persons need to be maintained for each project to evidence compliance.
Authorised Persons are those staff members that have some form of approval to access ITAR and/or EAR controlled technology.

**ITAR**
- All Defence staff can access ITAR and EAR as they are the ‘end users’. APS staff are different.
- Security Clearance
- Nationality called out in a TAA
- Vetted using 126.18 guidance on vetting

**EAR**
- Generally, a regular employee (not a contractor) is authorised. Above the line defence contractors can also generally access, but those below the line must be approved separately.

**AU Controls**
- None needed. Does not need to be your employee. Anyone in the physical territory of Australia.
About the International Traffic in Arms Regulations (ITAR)

- The International Traffic in Arms Regulations is a set of US regulations that strictly control access to certain sensitive technologies (mostly military, certain dual use articles).
- ITAR controlled technology is listed on the U.S. Munitions List (USML).
- The hardware, software and technical data listed on the USML are collectively referred to as ITAR “articles”.
- Where you have an ITAR article and you want to give someone access to it, retransfer it to another party, re-export it, exhibit it, sell it, etc. you will need State Department approval.
- Any Australian produced hardware, software or technical data that incorporates ITAR controlled technology will itself become subject to the ITAR. This is referred to as “ITAR taint”.
- Only persons authorised to receive or access ITAR controlled articles, including technical data may do so. Access by Unauthorised Persons is a violation of the ITAR.
- Violation of the ITAR can lead to very serious consequences, including U.S. government audits.

About the Export Administration Regulations (EAR)

- Technology of U.S. origin that is not controlled by the ITAR is controlled by the Export Administration Regulations (EAR). The EAR controls both military and commercial goods.
- EAR controlled technology are listed on the Commerce Control List (CCL)
- Any Australian produced hardware, software or technical data that incorporates over a certain threshold of EAR controlled technology will itself become subject to the EAR.
- The Bureau of Industry and Security (BIS) only issues one approval called a ‘license’.
- A new license may be required to share EAR controlled technology with a subcontractor or business partner in Australia or re-export EAR controlled technology to any destination other than the U.S.
- Most re-exports and retransfers in Australia can occur without a license, but you MUST check whether or not you need one.
- Recordkeeping is key to compliance and evidencing compliance.
- Access by unauthorised persons is a violation of the EAR
About Australian Export Controls

- Australia controls cross-border exports. Unlike the U.S. regulations, our Australian legislation is not extra-territorial.
- Australia controls hardware, software and technical data.
- Australia’s control list is called the Defence and Strategic Goods List or DSGL.
- You must have approval from Defence Export Controls (DEC) in order to export an item listed on the DSGL. There are many types of approvals, depending on the technology and the commercial circumstances.
### About the FMS Program

**Foreign Military Sales Program (FMS Program)**

- FMS an exemption in the ITAR (126.6)
- It can be used to export from the U.S. both ITAR and EAR controlled defense assets.
- FMS is a procurement methodology, not an export control regulation.
- EAR and ITAR can both be exported from the US (together) under the FMS exemption (126.6) in the ITAR. EAR must be managed as EAR even when it comes in this way.
- To give FMS procured assets to industry, the SPO needs a Third Party Retransfer Agreement (TPR) or other authority from the U.S. State Department.
- FMS assets have special rules around their transfer to other parties and destruction
- FMS is managed by PM/RSAT, not DDTC. Both are State Department agencies.

### MOUs

**Memorandum of Understanding (MoU) is**

- Basic understanding of what to governments are trying to achieve by cooperating with each other to produce a piece of military technology, such as the JSF.
- Outlines objectives of program and definitions of key terms
- Details responsibilities of each party (governments)
- License applications for export still required, but will be expedited
- Each participant must have a contact in place to legally bind contractors and subcontractors to not retransfer or use export controlled information for a purpose other than that specified by the MoU.
- Transferring export-controlled information must be in compliance with all applicable export control regulations of the participating countries.
LoAs

**Letter of Offer and Acceptance (LoA) is how an FMS contract is executed**

- Has Standard Terms and Conditions under which recipients must agree to use U.S.-provided defense articles, training, and services only for their intended purpose;
- **Recipients agree** not to transfer title to, or possession of, any defense article or related training to anyone not an officer, employee, or agent of that country or of the USG without prior written consent of the USG;
- **Recipients agree** to maintain the security of any article with substantially the same degree of protection afforded to it by the USG;
- **Recipients agree** to permit observation and review by, and to furnish necessary information to, representatives of the USG with regards to use of such articles.
- End Use Monitoring provides USG oversight to ensure these conditions are met (Golden Sentry Program)

---

TPRs

**Third Party Retransfer Agreements (TPR)**

**Basics about TPR**

- Under U.S. requirements associated with export control of FMS articles, it is only the Commonwealth (the SPO) 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 industry party must approach the Commonwealth (SPO) 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.

- TPRs can only be amended for 12 months post-execution. After this date has passed a new TPR is required or another authority must be sought.
How did the technology come to you?

ITAR

DDTC Approval

DCS

FMS

126.6

PMRSAT

TPR

EAR

126.6

PMRSAT

TPR

BIS License

DCS

MANAGING EXPORT CONTROLLED TECHNOLOGY FOR EFFECTIVE COMPLIANCE
Receipt and Marking

Upon receipt, Export Controlled Technology is segregated and logged it into the system including supplier, approval, jurisdiction, classification.

Ensure export controlled technology is marked as such

- On documentation itself so that it appears when printed (header, footer, cover page)
- In the file name/folder name
- On manuals and accompanying documentation such as invoices
- At the beginning of an email or in the subject line
- Mark all applicable controls (e.g. EAR and DEC)

Transferring/Retransferring

Where export controlled technology is leaving our facilities, and going to another place in Australia or into the custody of another entity you must:

- Ensure you have an approval in place
- Record which entity you are sending it to / granting access to
- Notify the other party of the jurisdiction and classification
### Storage and destruction

**ITAR**
- Store in a secure location/on a secure server to preclude access by Unauthorised Persons
- If acquired DCS, ask DDTC for approval to destroy, complete and witness certificate of destruction, retain for 5 years.
- If acquired FMS, PM/RSAT needs to give the approval for destruction. Your SPO’s authorised representative will contact IEC with questions.

**EAR**
- Store in a secure location to preclude access by contractors (unless authorised on a license or exception)
- Create a destruction certificate and retain for 5 years

**AU**
- No storage requirements as long as it is in AU
- No destruction certificate required

### Keeping Records

Each of the regulations has different record-keeping requirements, but in general keep:
- Records of receipt
- Records of transfer to another entity in Australia or overseas
- Records of access (ITAR and EAR)
- Lists of Authorised Persons (as updated) for each project
- Classification and Jurisdiction of all export-controlled technology
- Classification changes and Jurisdiction changes
- Copies of all approval applications (and supporting documentation)
- Copies of all approvals
- Destruction Certificates
- De Minimis calculations (EAR) and ITAR taint determination (ITAR)
Common ways to mismanage export controls

➢ ‘Exporting’ without a license or other approval. This includes stepping out of scope of an existing approval.
➢ Violating the terms and conditions of an approval
➢ Inadvertently providing access to an Unauthorised Person
➢ Misuse of or failing to make records of your use of exceptions/exemptions

Keys to effective compliance

Review documented Policies and Procedures

A list of Authorised Persons

Sufficient training for staff handling export controlled technology

Actively managing the SPO’s Export Compliance Management Program, including:

♦ ensuring access is only granted to Authorised Persons,
♦ reviewing contract clauses to ensure export controls responsibilities are communicated,
♦ conducting internal audits to verify compliance,
♦ handling compliance issues,
♦ ensuring record-keeping is sufficient and
♦ ensuring approvals are still valid and descriptive of the work being undertaken.
THANK YOU!