

US EXPORT CONTROLS

9-11 June 2015

The ITAR 'Virus' EARvolves!

SQUIRE
PATTON BOGGS

EGAD
Export Group for Aerospace & Defence

**STRATEGIC SHIPPING
COMPANY LIMITED**

ITAR and EAR Contamination and Impacts on Employment, Facility Visits and Retransfers

George N. Grammas

Partner and Chair, International Trade / Global Import and Export Compliance

Squire Patton Boggs (US) LLP

2550 M Street, N.W.

Washington, DC 20037

+1.202.626.6234

george.grammas@squirepb.com

ITAR and EAR Contamination: Extraterritorial Application of US Export Controls

ITAR and EAR Contamination and Impacts on Employment, Facility Visits and Retransfers (1.25)

- When and how does contamination occur
- What is the impact on non-US organizations
- Best practices to comply with ITAR and EAR after contamination

ITAR Contamination: Defense Articles

- Definition

§ 120.6 **Defense article.** *Defense article* means any

- Item or technical data designated in § 121.1 (USML)
- Includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in § 121.1

- Observation

- Includes US and non-US made items
- Not all defense articles are controlled by the ITAR
- When are non-US made defense articles subject to the ITAR

ITAR Contamination: Retransfer Controls

- Retransfer control statement
 - § 123.9 Retransfer/reexport. Control statement on all invoices
- DDTC approval required to:
 - Transfer non-US products containing US content
- Exemption: (§ 123.9 (e))
 - Reexports or retransfers of US-origin components incorporated into a foreign defense article to NATO, NATO agencies, a government of a NATO country, or the governments of Australia, Israel, Japan, New Zealand, or South Korea
 - Previously authorized for export from the United States
 - Not SME, not MDE worth more than \$25 million, not defense articles / services sold under a contract in amount \geq \$100 million, not identified as MTCR items
 - Reexporter must notify DDTC within 30 days of reexport
 - Not restricted from retransfer or reexport in original export authorization

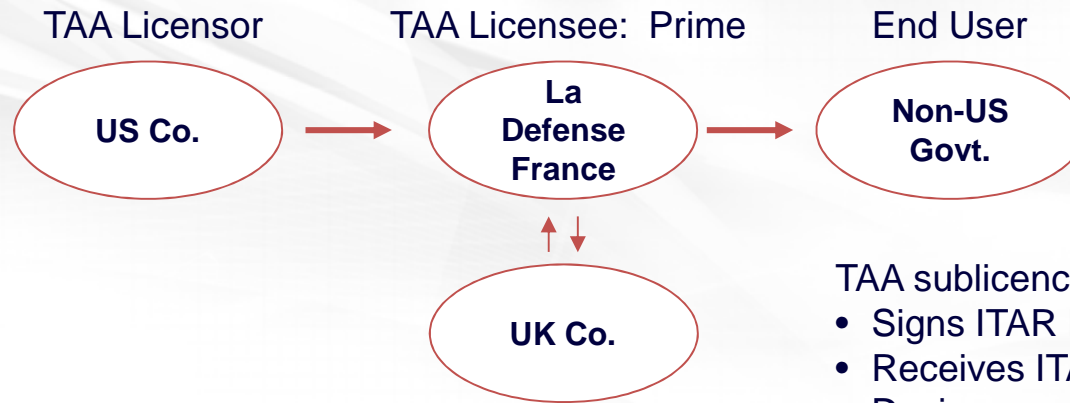


“These commodities are authorized by the U.S. Government for export only to [country of ultimate destination] for use by [end-user] under [license or other approval number or exemption citation]. They may not be resold, diverted, transferred, or otherwise be disposed of, to any other country or to any person other than the authorized end-user or consignee(s), either in their original form or after being incorporated into other end-items, without first obtaining approval from the U.S. Department of State or use of an applicable exemption.”

ITAR Contamination: Retransfer Controls, § 124.8(5)

- Required provision in a technical assistance agreement
 - “The technical data or defense service exported from the United States in furtherance of this agreement and any defense article which may be produced or manufactured from such technical data or defense service may not be transferred to a foreign person except pursuant to § § 124.16 and 126.18, as specifically authorized in this agreement, or where prior written approval of the Department of State has been obtained.”
- DDTC approval required to:
 - Retransfer of technical data received under a TAA
 - Transfer of defense articles (products or data) produced with the technical data received under a TAA
 - Except:
 - § 124.16 – EU / NATO+ employees of signatories and sublicensees
 - § 126.18 – employees of signatories of sublicensees subject to security clearance plan
 - As specifically authorized in this agreement (e.g., retransfer to end-user)
 - Where prior written approval of the Department of State has been obtained

ITAR Contamination: TAA Example



TAA sublicensee:

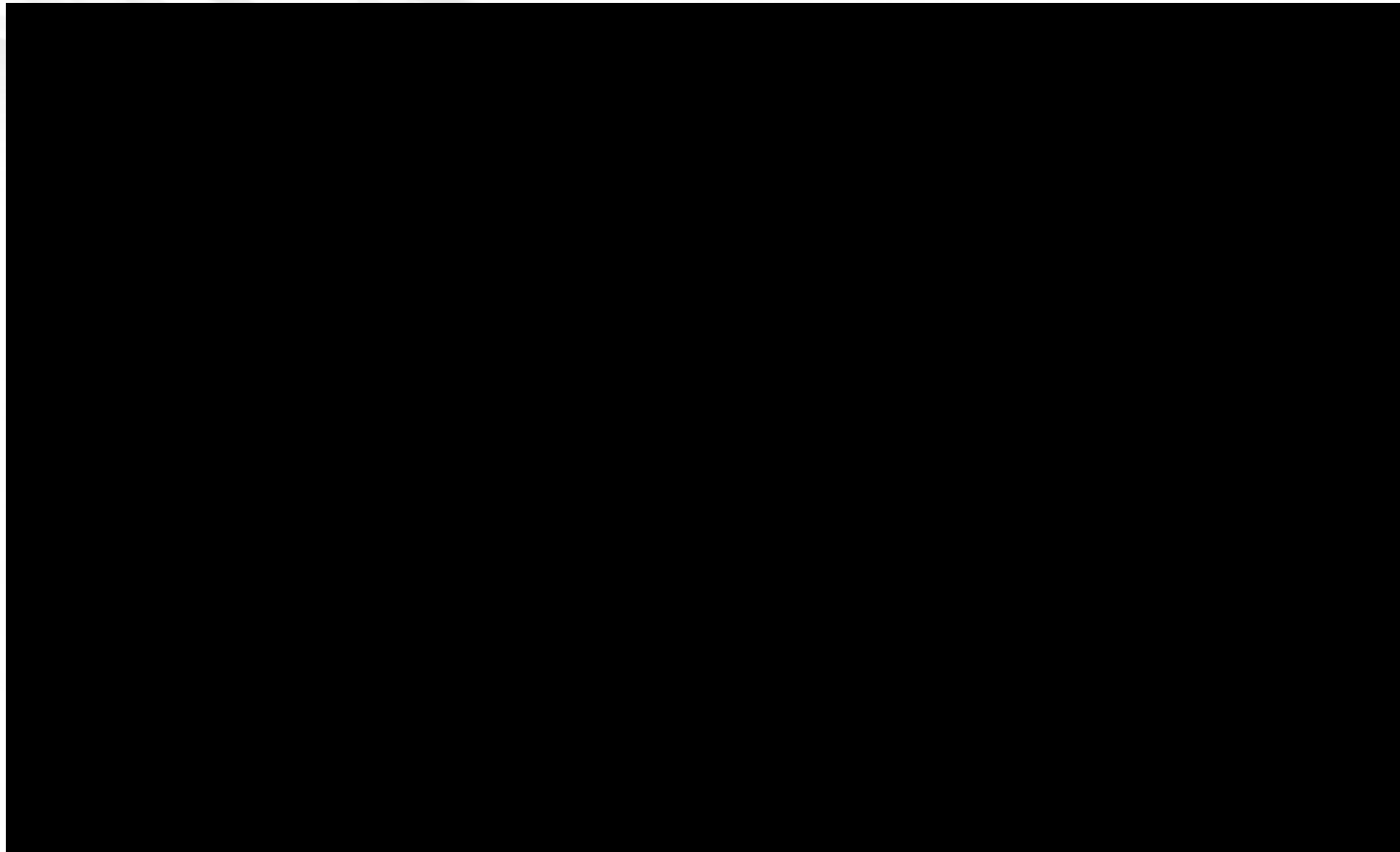
- Signs ITAR NDA that flows down 124.8 provisions
- Receives ITAR data
- Designs and builds system
- Uses various subcontractors

- Non-US signatories—all entities that have direct technical interchange with a US party
- Sublicensees—non-US entities having technical interchange with a TAA licensee only
 - TAA must describe roles of the sublicensees and the technical data to be retransferred to the sublicensee
 - Sublicensee must be listed in TAA, sign NDA and be in territory of the TAA
- End-User—in some (not all or most) cases, non-US government is a TAA party

When and How Does ITAR Contamination Occur?

Case Study

UK company receives technical data from the French company, La Defense, that signed a TAA. Is the UK business contaminated with the ITAR?



EAR Contamination: Scope of EAR (§ 734.3(a))

- All items in the United States
- All US origin items wherever located
- Foreign-made items that incorporate controlled US- origin item
 - Unless the controlled US content qualifies as de minimis
- Foreign-made direct products of US origin technology or software, provided:
 - Direct product is controlled for NS reasons; and
 - Technology or software is controlled for NS reasons

The term "direct product" means the immediate product (including processes and services) produced directly by the use of technology or software
- Certain commodities produced by any plant or major component of a plant located outside the United States that is a direct product of US-origin technology or software, provided:
 - Direct product of plant is controlled for NS reasons; and
 - Technology or software is controlled for NS reasons (TSR written assurances)

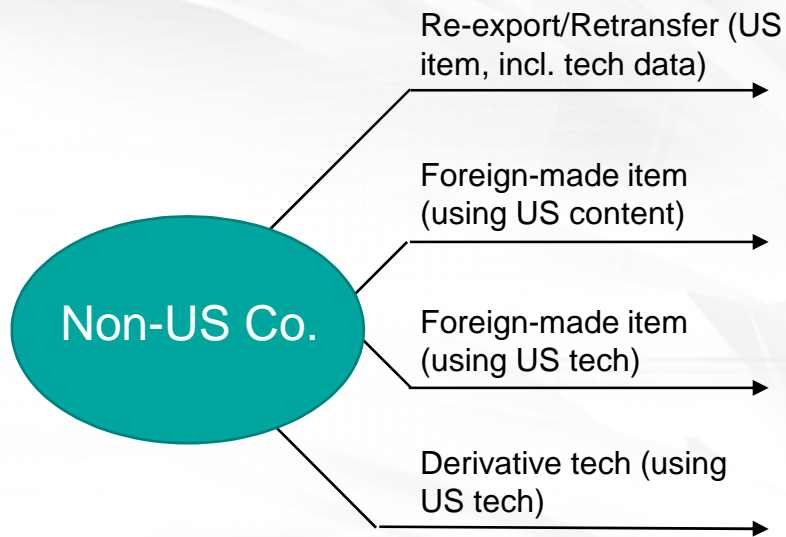
EAR Contamination: Excluded from Scope of EAR (§ 734.3(b) and § 734.7)

- Items that are exclusively controlled for export or reexport by other agencies: DDTC, OFAC, NRC, DOE, PTO
- Publicly available technology and software (except encryption software under 5D002)
 - Information is "published" when it becomes generally accessible to the interested public in any form, including
 - Publication in periodicals, books, print, electronic, or any other media
 - Ready availability at libraries
 - Patents and open (published) patent applications
 - Release at an open conference, meeting, seminar, trade show, or other open gathering
 - Software and information is published when it is available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution

EAR Contamination: De Minimis Rule (§ 734.4)

- General Rule:
 - If the foreign-made item is destined for Cuba, Iran, Syria, Sudan or North Korea, the US controlled content is de minimis if it is valued at 10% or less of the total value of the foreign-made item
 - If the foreign-made item is destined for any other country, the US controlled content is de minimis if it is valued at 25% or less of the total value of the foreign-made item
 - Compare hardware to hardware, software to software and technology to technology; do not sum US hardware, software and technology content
- 600 Series Rule:
 - There is no de minimis level for foreign-made items that incorporate US-origin “600 series” items when destined for a country listed in Country Group D:5 (ITAR 126.1 countries)
- Certain exclusions and limitations:
 - No de minimis for certain: high-performance computers, encryption technology, 9E003 technology and 6A003 items.
 - Special rules and requirements for encryption
 - Must submit a one-time report on de minimis calculation for technology

ITAR and EAR Contamination



**ITAR
Controlled**

**EAR
Controlled**

Yes

Yes

Yes

Only if > de minimis

Yes

Only if NS controls

Yes

Only if > de minimis

Requires prior approval
For example, DSP-5, TAA, WDA, GC Letter

License, license exception or NLR

ITAR and EAR Contamination: Extraterritorial Application of US Export Controls

- When and how does contamination occur
- **What is the impact on Non-US organizations**
- Best practices to comply with ITAR and EAR after contamination

What Constitutes a Re-export or Retransfer of Technology or Technical Data?

- Sending or taking **technical data** to another country or to another non-US person
 - Includes
 - Sending technical data recorded or stored in any physical form
 - Sending via fax or email
 - Access via servers or websites
 - Telephone calls
- Disclosing technical data, including visual or oral access to technical data, to a dual national or third country national (DN/TCN)
 - This is called a **deemed re-export**
 - DN/TCN = dual-national / third country national
- Providing technical assistance to another company or to a DN/TCN
 - This is called a **defense service** if the assistance relates to a defense article
- EAR definition
 - “Technology” takes the form of “technical data” or “technical assistance”

What Is a Deemed Re-export?

- Employment of DN/TCN
- Facility visit by DN/TCN
- Other interchanges with DN/TCN



Deemed Re-export

- Release of **technical data** to a **DN/TCN** is “deemed” to be an export to the foreign person’s “**home country**” on the assumption that the foreign person may return to their home country and disclose the technology.

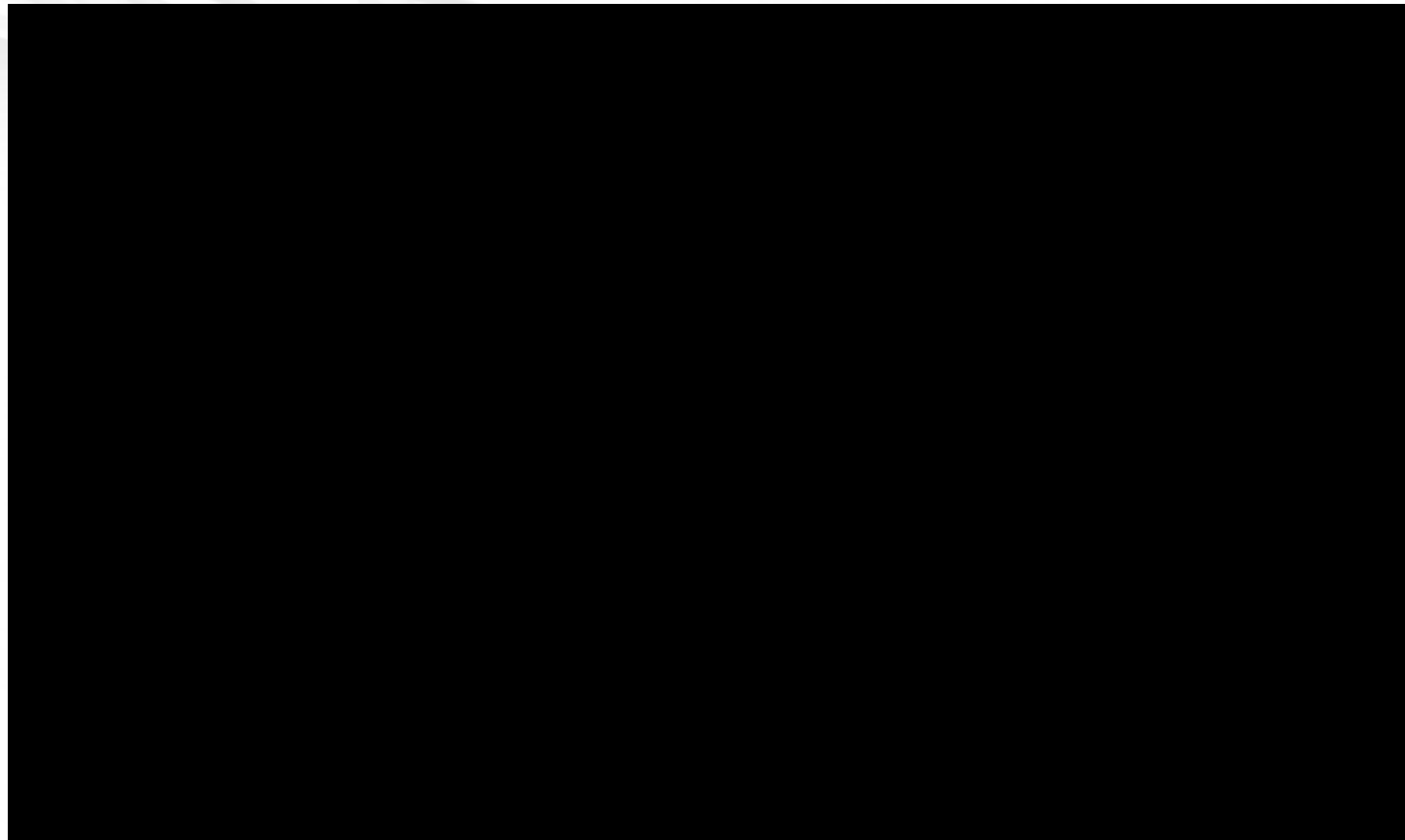
Home Country: ITAR vs. EAR

- Home Country
 - ITAR. Citizenship, place of birth, AND place of issuance of passport
 - EAR. Most recent: citizenship OR place of permanent residence
 - Circumstances may exist where the last place of citizenship or permanent residence is unclear or obscured by other facts, and in these cases, the last in time rule possibly should not be used
- Under ITAR, person can be of more than one nationality
 - The term “Dual National” means an individual who holds nationality from the country of the employer/facility and also holds nationality from one or more additional countries
 - The term “Third Country National” means an individual who holds nationality from one or more countries, but does not hold the nationality of the employer/facility
- Under EAR, person can be a TCN (i.e., a national of another country)
 - Generally, cannot be a dual national under the Commerce last in time test

Note: A US Person is always a US Person, not a FP because DN.

Impact of Contamination: Employment Problem

UK company receives technical data from a French company that signed the TAA. How does this impact employment of personnel at the company and its vendors?



Employment of DN/TCNs

- Access to manufacturing facility
- Access to technical documents
- Access to engineering database and other stored data
- Discussions and meetings with other employees
- Options:
 - Authorize the employees
 - Lock out the unauthorized employees
 - Lock down the ITAR and EAR controlled technical data



What Is Technical Data?

- Technical data is specific information that is ***necessary or required*** for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of an article.



Technical data is not:

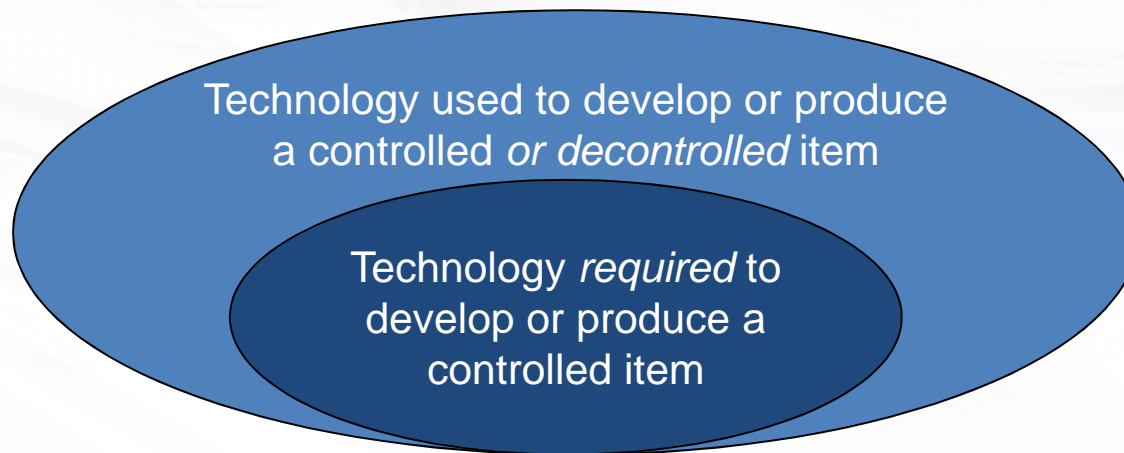
- Basic marketing info, conceptual info, general descriptions
- Fundamental research
- Under the EAR, publicly available information

Technical data is:

- Detailed product info including detailed requirements
- Detailed interface info including detailed ICDs, ATPs
- Detailed design and manufacturing data including design, formulation, process
- Know-how

Determine Applicable Technical Data Controls

- Follow the designation of the data as provided by the exporter for data received from the US
 - If marked ITAR, the data and all derivative works should be treated as ITAR controlled
 - If marked EAR, the data and derivative works can be classified as follows:
 - Technology that is common to a controlled and decontrolled product and not specifically required for the development, production, or use of a controlled product is not controlled
 - Technology that is required for the development, production, or use of a controlled product remains controlled even when applicable to a product that is controlled at a lower level

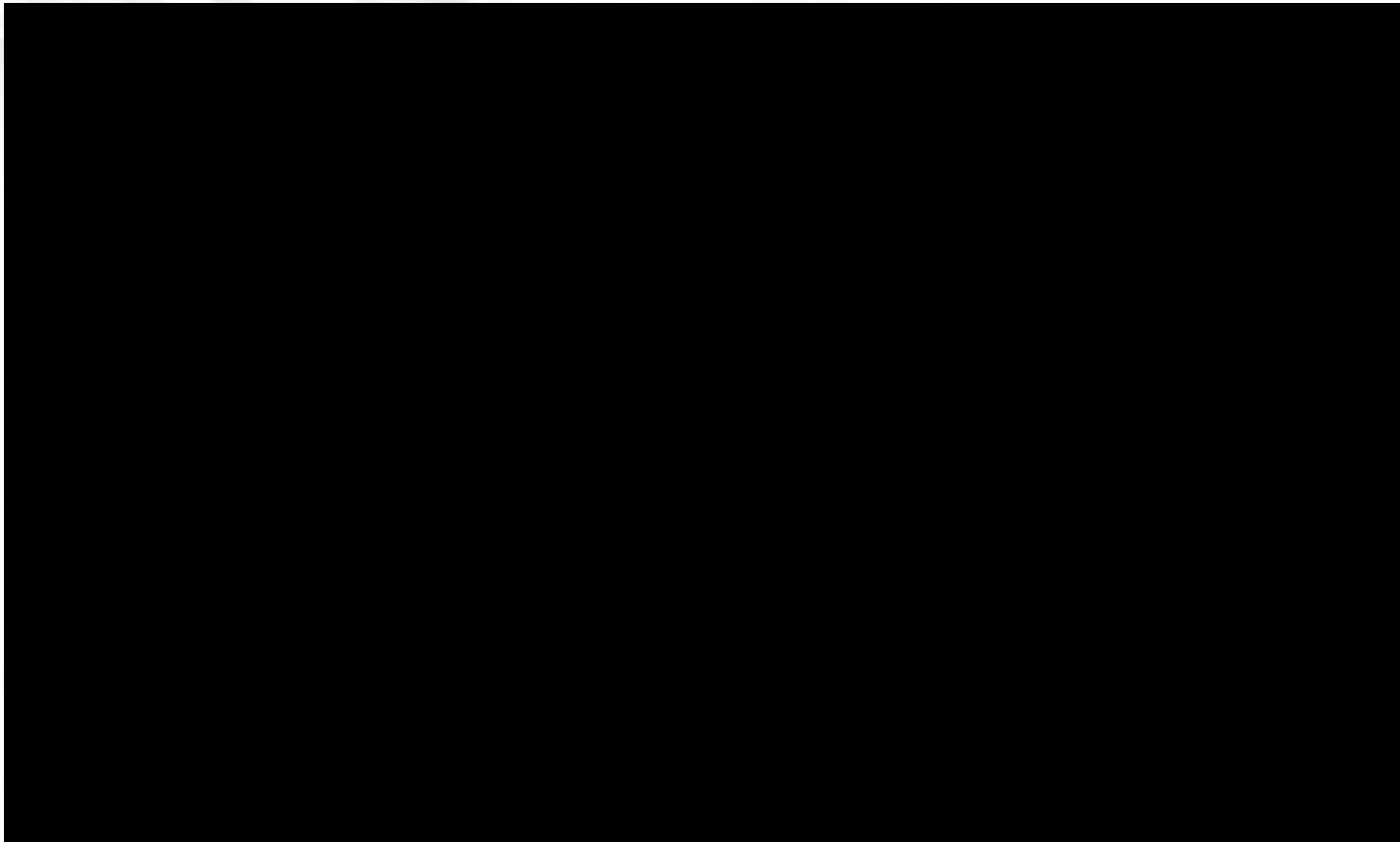


Some *Possible* Examples of Technical Data

- Engineering database
 - Bill of materials
 - Manufacturing process steps for costing
 - Drawings
 - Instructions for production
 - Work breakdown schedule
 - Materials list
 - Testing procedure
- Application database
 - Customer requirements and interface data
 - Customer system operation data
 - Technical comparison of products or competitors

Impact of Contamination: Facility Visit Problem

UK company receives technical data from a French company that signed the TAA. How does this impact visits at the companies facilities?



Facility Visits by DN/TCNs

- Observation of defense article at different points of production
- Observation of manufacturing process
- Observation of manufacturing equipment
- Technical presentation Discussion
- Options:
 - Authorize the visit
 - Limit the tour and discussions



Contamination Problem Review: Evaluation in the US

- You send a UK-made military aircraft electronics kit to the US for testing and evaluation. The product is ready to be returned to the UK
- Assume item is on the USML
 - Do you need a DDTC license to return the electronics to the UK?
 - (a) No. The product is UK made and is covered by UK export legislation.
 - (b) Yes. The product is a defense article and ITAR-controlled.
 - (c) Depends. Only if the product was modified in the US.
- Assume item is on the CCL
 - Do you need a BIS license to return the electronics to the UK?
 - (a) No. A license is not required for CCL items.
 - (b) Yes. A license is always required for CCL items.
 - (c) Depends. If so, on what?

Contamination Problem Review: Hardware Modification for USAF Compatibility

- The US company sends you integrated circuit board (ICB) to integrate into your kit so that it will interface with the USAF platform
- Assume the ICB is on the USML
 - Is your kit after ICB integration subject to the ITAR?
 - Do you need to control access to the ICB or the kit after integration?
 - Do you need to control access to installation and test documentation on the ICB?
- Assume the ICB is on the CCL
 - Is your kit after ICB integration subject to the EAR?
 - Do you need to control access to the ICB or the kit after integration?
 - Do you need to control access to installation and test documentation on the ICB?

Contamination Problem Review: Technical Modification for USAF Compatibility

- The kit does not interface properly with another component. The US company assists in troubleshooting the problem, which ultimately results in calibration of the kit and minor modifications to avoid RF interference.
- Assume the technical data and defense service are on the USML
 - Is your kit now subject to the ITAR?
 - Do you need to control access to the production process or the kit?
 - Do you need to control access to revised design and production documentation?
- Assume the technology (assistance) is on the CCL
 - Is your kit now subject to the EAR?
 - Do you need to control access to the production process or the kit?
 - Do you need to control access to revised design and production documentation?

Is Access to Data an Export?

- Is access a violation of the ITAR (or EAR) or is an actual transfer required?
- 2004 Consent Decree (State) – General Dynamics and GM agreed to US\$20 million in civil penalties and remedial compliance measures
 - Foreign persons had computer access to databases and servers containing technical data related to ITAR-controlled light-armored vehicles at GM
 - Reliability and maintainability data
 - Engineering drawings and manufacturing information
 - Foreign person status was not checked prior to access
 - Proposed charges were based on disclosing or transferring controlled technical data to foreign persons without authorization (ITAR Section 127.1)
- February 2014 Settlement (BIS) – Intevac agreed to pay US\$115,000 to settle deemed export charges
 - California-based company released to a Russian national employee technology for hard disk drive manufacturing controlled for national security reasons
 - Release occurred by providing passwords and login information to the employee to access U.S.-based servers where data was stored, which allowed employee to view, print and create attachments to controlled tech data stored on the servers

IT Access

- Server
 - Location of server
 - Access to controlled data in files
 - Access to controlled data in database
 - Nationality of administrators
- In the consent agreement, UTC agreed:
 - To conduct a study to identify feasible enterprise improvements to maximize automation of the identification and tracking of ITAR-controlled technical data throughout respondent's information technology infrastructure and otherwise safeguard ITAR-controlled data against unauthorized access within that infrastructure. On the basis of this study, respondent will propose a plan to implement measures that will track, control, and record access to ITAR-controlled technical data by all users, including transfers onto laptops and portable storage devices, consistent with foreign privacy laws and any other technology or legal limitations. (Emphasis added)

ITAR and EAR Contamination: Extraterritorial Application of US Export Controls

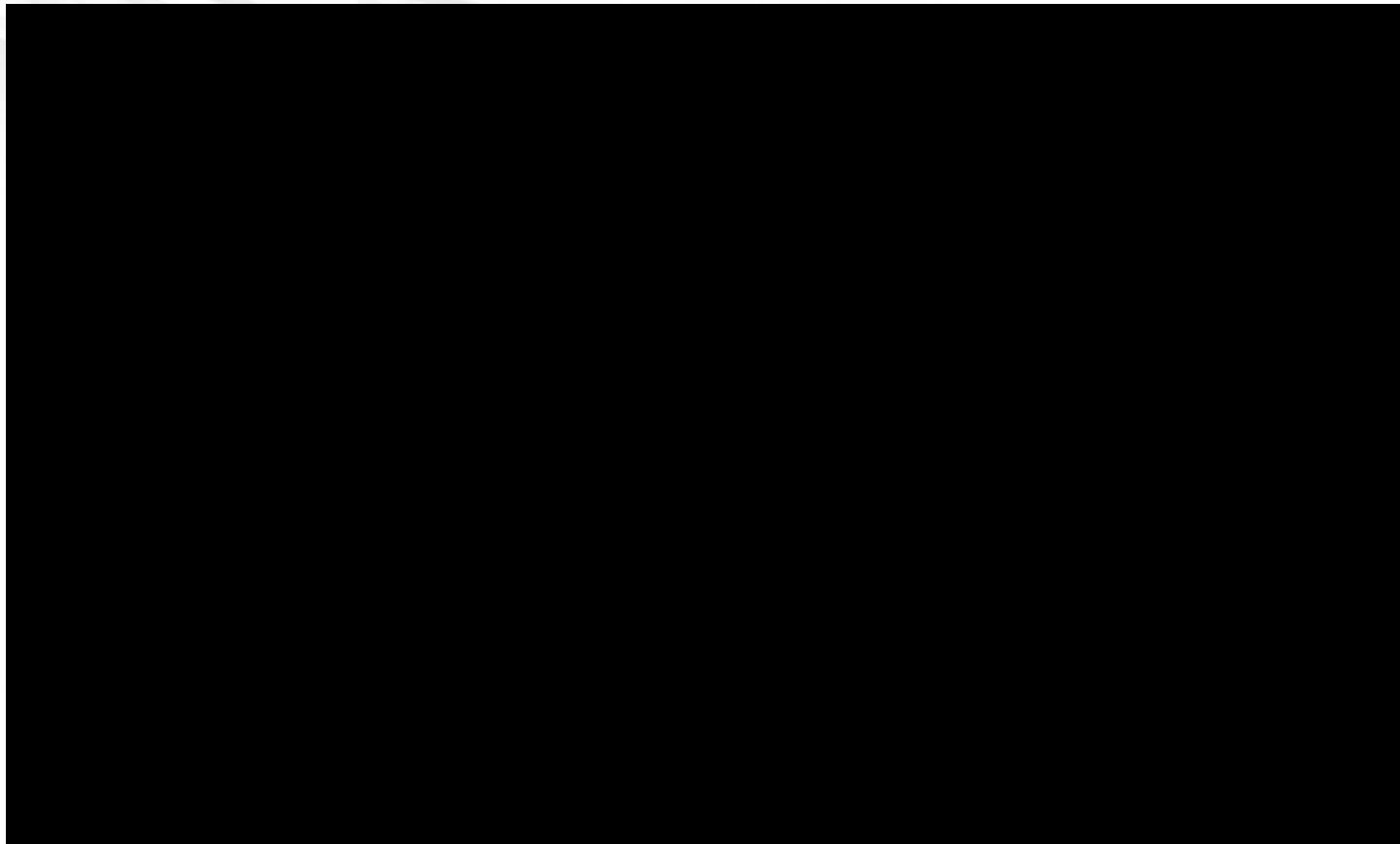
- When and how does contamination occur
- What is the impact on Non-US organizations
- **Best practices to comply with ITAR and EAR after contamination**

Confirm Proper Export Jurisdiction and Classification Decisions by US Supplier

- Consider the impact on you if the US supplier classified the ICB and technical assistance as ITAR controlled when actually under the EAR
 - Some suppliers treat everything as ITAR controlled
 - Supplier may not be familiar with export controls reform
- Consider the impact on you if the US supplier classified the ICB and technical assistance as EAR controlled when actually under the ITAR
 - Some suppliers are not familiar with the ITAR because mostly in non-military business or do not understand that a legacy product can remain subject to the ITAR until it is removed by CJ determination
- Which case is worse?

Commodity Jurisdiction: Ferry Boat Radar Example (cont.)

If the US company made a mistake on the export jurisdiction, who has a problem?



Implement Procedures to Identify and Contain ITAR and EAR Content

- Require that customers, vendors and partners advise you of any information that they deem to be ITAR-controlled and EAR-controlled technical data, hardware and software
 - Unmarked = EAR99 or AT controls only
- Implement procedures for handling, exporting and transferring controlled products
 - Confirm availability of license, ITAR exemption or EAR exception
- Implement procedures for handling, exporting and transferring products that do not require prior approval
 - Sanctioned or embargoed countries
 - Denied or restricted parties
 - Proscribed end-uses
 - Diversion “red flags”
 - Participation in unsanctioned foreign boycotts
- Implement internal technology control plan
- Train employees

Internal Technology Control Plan – Physical Controls

- Limitations on physical access/security
 - Segregated work areas
 - Badges: indicating credentials and access rights or access restrictions
 - Escorts for DN/TCN persons in restricted areas
- Hardcopy document controls
 - Secure storage
 - Limited release/distribution legends
- Administration
 - DN/TCN person indoctrination
 - DN/TCN employee database: visa, export license, scope
 - Facility visit request form: purpose and scope of visit
 - Supervisor/host accountability of foreign person employees/visitors
 - Training and written certifications / acknowledgements

Internal Technology Control Plan – Virtual Controls

- **Emails**
 - Avoid sending controlled technical data over the Internet by email
 - Prefer controlled technical data to be downloaded over secure connection to server
 - Mark files and emails (in subject heading) containing controlled technical data
 - Certify exports with exemption or license
 - Create a data “drop box” to keep a record of controlled data exports
 - Distinct email addresses for foreign person employees
- **Travel with “clean” laptops and Blackberry devices**
 - Download data after arriving
 - Erase before traveling between countries
 - Consider using HTML tool to read data without downloading to laptop (rather than VPN which will transfer inbox to laptop)
- **Servers**
 - Design firewalls and password controls to protect folders and files
 - Limit network access for foreign person employees
 - Maintain US-controlled technical data on a US-based server

US EXPORT CONTROLS

9-11 June 2015

The ITAR 'Virus' EARvolves!

SQUIRE
PATTON BOGGS

EGAD
Export Group for Aerospace & Defence

**STRATEGIC SHIPPING
COMPANY LIMITED**

ITAR and EAR Contamination and Impacts on Employment, Facility Visits and Retransfers

George N. Grammas

Partner and Chair, International Trade / Global Import and Export Compliance

Squire Patton Boggs (US) LLP

2550 M Street, N.W.

Washington, DC 20037

+1.202.626.6234

george.grammas@squirepb.com