Facing the Tech Data Challenge

John Black
BSG Consulting
February 13, 2013
Introduction

- Speaker: John Black, BSG Consulting

- Objectives:
  - Analyze key tech data compliance issues & challenges—more issue oriented than analyzing the regulations, but analyze some key aspects of the rules.
  - Discuss approaches for compliance
  - Consider priorities, objectives and methods for achieving compliance

- Do not expect to receive easy, painless solutions to the challenges of old fashioned and burdensome US export/reexport controls
Key Issues We Will Not Cover

- Detailed technology classification
- Basic EAR license determination
- Focus on your industry-specific issues
- Types of licenses and approvals for technical data
Initial and Ongoing Tasks

- Conduct an initial & continuing self assessment:
  1. Find & classify your inventory of tech data
  2. Find all of your methods of export/reexport. Put in place compliance procedures for each method

- Assign priorities based on a risk assessment. Start with the highest risk—examples of risk factors:
  - Sensitivity of tech data and countries
  - Likelihood of violation
  - Likelihood of government detecting violations
Initial and Ongoing Tasks

1. Find, identify and classify your inventory of tech data and software

   Find & Identify
   • What type of information are we looking for
   • What are we not looking for?
   • Where are we likely to find what we are looking for?

   Classify It
   • Is it subject to US jurisdiction?
   • USML and CCL jurisdiction/classification
   • Identify controlled technology
**EAR**

"Technology"—Specific information necessary for the "development", "production", or "use" of a product. The information takes the form of "technical data" or "technical assistance".

"Technical data".—May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

**ITAR**

§ 120.10 Technical data.

(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;

(3) Information covered by an invention secrecy order;

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

(5) This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain as defined in § 120.11. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.
What is NOT technical data/technology?

- Does not include:
  - ITAR “public domain”
  - EAR “publicly available”
  - ITAR “basic marketing”
  - ITAR “general system description”
  - Science/engineering principals

- We will not examine the nuance differences between EAR and ITAR definitions here
§ 120.11 Public domain. (a) Public domain means information which is published and which is generally accessible or available to the public:

(1) Through sales at newsstands and bookstores;
(2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;
(3) Through second class mailing privileges granted by the U.S. Government;
(4) At libraries open to the public or from which the public can obtain documents;
(5) Through patents available at any patent office;
(6) Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;
(7) Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency (see also § 125.4(b)(13) of this subchapter);
(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:
   (i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or
   (ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.
**ITAR “Public Domain” Issues**

- On December 6, 1984, the State Dept. published a notice in the Federal Register so that the ITAR no longer requires that you obtain US Government authorization to put your technical data in the “public domain”

- In that Federal Register notice, the State Dept. said, “A provision has been added to make it clear that the regulation for the export or technical does not purport to interfere with the First Amendment rights of individuals.”

*If the drafters intended that prior US Government approval was required for placing all defense information into the Public Domain, they would have explicitly written that. Why are we so sure? Because at one point, the ITAR did just that: it explicitly required prior approval for publishing public information. The drafters explicitly dropped this requirement in 1984, citing First Amendment and other concerns.*

**1969 ITAR:** The 1969 version of the ITAR, which governed defense exports through 1984, did not mention “Public Domain.” Instead, the definition of technical data included a wide variety of defense information as does today’s ITAR, but without any exclusion for Public Domain information. The 1969 ITAR offered a published information license exemption as precursor to today’s Public Domain. The published information license exemption stated that Customs should permit the export of technical data without a license if it “is in published form and subject to public dissemination by being: (i) Sold at newsstands and bookstores; (ii) Available by subscription or purchase without restriction to any person or available without cost to any person, (iii) granted second class mailing [bulk mail] privileges by the US Government; or (iv) Freely available at public libraries.” This public domain-like exemption contained this footnote: “The burden for obtaining appropriate US Government approval for the publication of technical data . . . , including such data as may be developed under other than US Government contract, is on the person or company seeking publication.” The 1969 ITAR therefore explicitly required that publishing defense information is subject to some kind of US Government approval.

**1980 ITAR Proposed Revision:** Was the removal of this prior approval requirement from the modern ITAR a mere accident? No, according to the Supplementary Information section of Federal Register Notices for the modern version of the ITAR. In the proposed rule for a new ITAR issued on December 19, 1980, State introduced the concept of Public Domain information being excluded from the definition of technical data. The footnote requiring pre-publication approval was removed from the published information exemption. Why did the State Department do this? The Supplementary Information section of the Federal Register Notice illuminates: “A provision has been added to make it clear that the regulation for the export or technical does not purport to interfere with the First Amendment rights of individuals.”

Requiring prior approval for publication is a prior restraint on free speech that subjects any Federal regulation to heightened scrutiny under the US Constitution. In fact, in cases prior to the proposed rule, the Courts had cited that the First Amendment did apply to the ITAR.

**December 6, 1984 ITAR:** The final rule of the 1984 ITAR went one step further. It removed the published information exemption altogether, but placed the exemption language virtually verbatim into the definition of Public Domain, again minus the old footnote that required prior Government publication approval.
The importance of “publicly available” classification is that there are no export restrictions. If someone in Cuba downloads publicly available information from your public web page, there is no license requirement (or violation).

Supplement No. 1 to Part 734 includes many explanatory questions and answers that are intended to clarify “publicly available.”
Taking inventory is an ongoing process. Your company will continually develop new TD and SW and will continue to keep it in new places and have new opportunities for export.

Your compliance procedure should assign to you or somebody else the responsibility for classifying new TD and SW and identify new opportunities for export. This means export compliance must insert itself into new programs and projects.
TD & SW Compliance Tasks *(Revisited)*

1. (Continued...) After you find it, classify it:
   - Determine USML/CCL jurisdiction and classification
   - If outside the United States, determine what TD and SW is US-origin or has US content
   - Sometimes you classify what it is *not*—“we do not have any ITAR data” OR “we do not have any data classified above 9E991 except xyz”

2. Identify export opportunities
   - Definition of “export”; concept of “deemed export”
   - Emerging issues re: TD and SW exports

3. Establish compliance procedures based on risks
“Foreign nationals” and “foreign persons” are persons who are not:

- US citizens,
- US permanent resident aliens ("green card holders"), or
- Other protected individuals (e.g., refugees, or have political asylum)

So, this means that a permanent resident alien (a.k.a. green card holder) is treated as a US Person for purposes of the deemed export rule, while persons who hold a temporary visa (such as a H1 work, tourist or student visa) are treated as foreign nationals for purposes of the deemed export rule.

The ITAR also applies its rules to transfers to companies incorporated outside of the United States and US citizens who are employed by companies incorporated outside the United States. The EAR focuses on nationality of the person rather than the company that employs that person. Transferring tech data to a US citizen employee of a company incorporated outside of the United States is a Red Flag.

For the EAR, if a person has more than one citizenship, you look at his country of most recent permanent resident or citizenship status (for example, a dual Syrian-Canadian citizen who was born in Syria who has lived in Canada for the last 10 years is treated as Canadian for EAR purposes.

For the ITAR, if a person has more than one citizenship, you consider that person to be both countries of citizenship.
“Foreign nationals” and “foreign persons” are persons who are not:

- US citizens,
- US permanent resident aliens ("green card holders"), or
- Other protected individuals (e.g., refugees, or have political asylum)

So, this means that a permanent resident alien (a.k.a. green card holder) is treated as a US Person for purposes of the deemed export rule, while persons who hold a temporary visa (such as a H1 work, tourist or student visa) are treated as a foreign nationals for purposes of the deemed export rule.

The ITAR also applies its rules to transfers to companies incorporated outside of the United States and US citizens who are employed by companies incorporated outside the United States. The EAR focuses on nationality of the person rather than the company that employs that person. Transferring tech data to a US citizen employee of a company incorporated outside of the United States is a Red Flag.

For the EAR, if a person has more than one citizenship, you look at his country of most recent permanent resident or citizenship status (for example, a dual Syrian-Canadian citizen who was born in Syria who has lived in Canada for the last 10 years is treated as Canadian for EAR purposes.

For the ITAR, if a person has more than one citizenship, you consider that person to be both countries of citizenship.

<table>
<thead>
<tr>
<th>Definitions of Export/Reexport=Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>“Deemed” Exports Issues:</strong> Release tech data in the US or abroad to</td>
</tr>
<tr>
<td>- A “foreign person” (ITAR—includes humans and entities incorporated outside of the United States) who have a nationality other than where located</td>
</tr>
<tr>
<td>- A “foreign national” (EAR—includes humans) who has a nationality other than where located</td>
</tr>
<tr>
<td><strong>How do you determine nationality, EAR vs. ITAR?</strong></td>
</tr>
<tr>
<td>- EAR—most recent country of citizenship or permanent residence</td>
</tr>
<tr>
<td>- ITAR—DDTC considers all countries of citizenship, country of origin, country of birth</td>
</tr>
</tbody>
</table>
Using Encryption to Mitigate Risks

- An export of encrypted tech data may be an export, according to the definitions.

- But if the encrypted tech data cannot be (or is not) accessed by the recipient, that is mitigation against more serious penalties for unauthorized exports. Examples:
  - I email encrypted ITAR tech data to my co-worker, not knowing he is in another country. My co-worker is trained not to decrypt the file overseas and no party overseas could access the encrypted tech data.
  - A foreign national gets access to encrypted ITAR tech data on our server. The FN does not attempt to decrypt.
Using Encryption to Mitigate Risks

- **Encryption should not be the foundation of your compliance program, but is a good second line of defense**

- Consider combining the use of encryption for tech data on servers, emails, laptops, etc. with other compliance policies and procedures

- People responsible for safeguarding your intellectual property likely are good allies to support implementation of data encryption policies such as encrypting emails
Using Encryption to Mitigate Risks

- You IT department likely has experts to help you design a workable and efficient approach.

- Using encryption raises issues related to compliance with encryption export, reexport, import, and use restrictions.
  
  - **US EAR Issues**: EAR has extremely complex but relatively relaxed export/reexport controls on encryption products.
  
  - **Foreign (i.e., Non-US) Rules**: Some countries have restrictions on import, export and use of encryption.
Issue Analysis

- Now that we understand:
  - What items (tech data) we are looking for
  - What activities (export/reexport) we are looking for

- We are ready to look at specific issues and challenges and consider options for compliance procedures
Deemed Export/Reexport Issues

- **Note:** *DDTC does not like its rules referred to as “deemed”*

- You may have issues with these people:
  - Employees
  - Visitors
  - Contractors
  - Service providers
Foreign Persons/Nationals

- **Foreign National Employees**
  - Compliance procedures for existing inventory of foreign national employees to prevent electronic, tangible and intangible access to technical data
    - Obtain export licenses
    - Access control plans—physical and electronic access
    - Training foreign national employees and all other employees
    - Encryption to mitigate risk?
  - **Evaluation and hiring new foreign national employees**
    - Develop routine questions for all potential new employees
    - Analyze export compliance issues before hiring
I-129 Deemed Export Certification

- **U.S. employers** must use a new version of the Form I-129, “Petition for a Nonimmigrant Worker”
- Must certify that it has reviewed the EAR & ITAR and has determined that either:
  1. A license is not required to release technology or technical data to the foreign person; or
  2. A license is required and the petitioner will prevent access to the controlled technology or technical data by the beneficiary until and unless the petitioner has received the required license

- **Not a new export license requirement**
Foreign Persons/Nationals

- Sample Foreign Visitors Procedure
  - Host of foreign visitor must obtain approval
  - Export compliance person does an export compliance review of foreign visitor request and issues approval (or denial) form which places restrictions and conditions on visit (e.g., visitor always must be accompanied, no access to test lab, release only technical data authorized on license D123456).
  - Approval goes to host and security guard/front desk
  - Visitors must identify nationality (personal nationality and company nationality) to security guard who won’t allow any foreign visitor without export approval
Foreign Persons/Nationals

- Sample Contractors/Service Providers Procedure
  - Require that the companies who are contractors or service providers promise not to send foreign nationals/persons to do work for you or at your facility—avoid making your company responsible for constantly assessing the nationalities of representatives of contractors/service providers
  - Include a standard clause in written agreements with all such companies
  - Find out who in your organization hires and monitors contractors and service providers
Cloud Computing: Who Is the Exporter?

- Cloud computing permits users to access data, software, applications and computer processing from the internet rather than from local hard drives or servers.
Cloud Computing: Who Is the Exporter?

- BIS advisory opinions: Cloud service provider is not the exporter under the EAR therefore does not have to obtain licenses/authorization for what is on the cloud. No similar DDTC written advice.

- Presumed responsibility for compliance lies with company/person who put tech data and software on the cloud or who provide defense services via the cloud
Cloud Computing: Who Is the Exporter?

BIS advisory opinions:

- Cloud service provider is not the exporter under the EAR therefore does not have to obtain licenses/authorization for what is on the cloud.
  - Presumed responsibility for compliance lies with company/person who put tech data and software on the cloud or who provide defense services via the cloud

- No similar DDTC written advice.
Cloud Computing: Who Is the Exporter?

BIS advisory opinions:

- Services without any exports (e.g., client software) NOT subject to the EAR unless involving missile tech, chem/bio

- Computational capacity NOT subject to the EAR unless missile tech, chem/bio
  
  - "the provider of computational capacity would not be considered to be the exporter under the EAR when the user exports data stored on the computational capacity or exports data resulting from use of the computational capacity"

No similar DDTC written advice.
Cloud: What are the compliance issues?

- You may export/reexport tech data and software via the cloud if:
  - foreign locations have access—location of the cloud and location of users
  - foreign nationals/persons have access—nationality of cloud staff/contractors and users
- You may have “defense service” issues if you provide controlled services to foreign persons—using computing power or software related to defense articles
- You may have issues if you provide cloud services to embargoed/sanctioned countries nationals
Cloud: Some Compliance Tasks

- **Assess the current state of your cloud:**
  - What is the current inventory of data & software on somebody else’s cloud. How is it classified (or how is it not classified—"We have nothing above 9E991")?
  - What people have access to what?
  - What locations have access to what?
  - Are their access controls/limitations in place?
  - In what country/countries is the cloud located?
Cloud: Some Compliance Tasks

- **Assess the current state of your cloud:**
  - What cloud services are we providing:
    - Computational access
    - Software as a service
    - Data storage
    - Other
  - And to whom are we providing such services
### Cloud: Some Compliance Tasks

- **Set policies and procedures for cloud:**
  - Develop overall cloud policy to prevent violations
  - Procedure to assess classification of items before they are put on cloud
  - Procedure for granting access to new persons/organizations/locations
  - Procedures to prevent license-required access when there is no license
  - Separate and secure cloud for controlled items?
  - Encryption?
Cloud Computing vs. Servers

- Servers present the similar compliance issues and require a similar approach as was discussed for cloud computing.

- The big difference is your company likely has its own servers and administers the servers.
Third Party Administration of Servers

- If you choose to use a third party to administer your servers, you may have export/reexport compliance issues:
  - Where is the third party located?
  - What are the nationalities of its employees with access to your servers?
  - What is on the servers and what is its classification?

- The third party and its employees likely will have unlimited access unless you get involved
US Tech Data, Foreign Tech Data, & Mixtures

- **Note:** “*Foreign*” = *non-US origin*
- Issue for multinationals and their partners
- All tech data and software (regardless of origin) in the United States is subject to US export controls when it is exported (including deemed exports) from the United States
  - Raises issues for foreign tech data and software stored in clouds or servers in the United States
  - Foreign tech data and software ceases to be subject to US control after it leaves the United States
  - Consider not using clouds or servers in the US as repositories for foreign tech data and software
US Tech Data, Foreign Tech Data, & Mixtures

- Foreign tech data changed, enhanced, or improved in the United States is permanently contaminated with US origin content
  - The contamination on the changed, enhanced, or improved data does not flow back to the original uncontaminated foreign origin data
  - Consider revisions tracking system that identifies which data is subject to what level of US jurisdiction and controls
US Tech Data, Foreign Tech Data, & Mixtures

- When a US and non-US company work outside of the United States to develop a new technology or technical data, such foreign tech data may be contaminated with US content.

- US rules control foreign data mixed with, drawn from, or derived from US tech data
  - EAR has 10% and 25% de minimis levels of control on foreign tech data so there is some escape from control
  - ITAR has control regardless of the amount of US ITAR content in foreign tech data
  - Remember Qioptic ITAR violation: “derivative data”
De Minimis Jurisdiction Levels

0% to 10% US Content = No US jurisdiction
>10% to 25% US Content = US jurisdiction for Cuba, Iran, North Korea, Sudan and Syria
>25% US Content = US jurisdiction for all countries

REPORT AND WAIT REQUIREMENT FOR TECHNICAL DATA

Supplement 2 to Part 734 tells you how to prepare and file the report and what information to use and report in calculating the percentages.

Once you file the report, you must wait 30 days. If you do not hear from the Commerce Department during the 30 days, you may proceed based on your de minimis calculations.

The 10% and 25% de minimis levels do not apply if:

- the US tech data is controlled by ECCN 9E003a.1 through a.12, and .f, and related controls, or controlled for “EI” reasons under ECCN 5E002; or
- the US software is encryption software controlled for “EI” reasons under ECCN 5D002
US Tech Data, Foreign Tech Data, & Mixtures

- Consider the implications of US jurisdiction and controls on foreign tech data developed, changed or enhanced with US input before you decide to engage in that activity.

- Companies need to put in place systems to identify, tag, and track tech data.
  - **Foreign companies:** Require their US partners to identify export classification. Then the foreign company should have a system to tag and track the US tech data and prevent unauthorized access.
  - **US companies:** Track foreign data in the US—changed?
Email Issues

- **Clear Issue**: Emails with tech data are exports if they go to a recipient in a foreign location or go to a foreign national

- **Lower Risk Potential Issues**: Email routing beyond the control of the sender
  - *Example*: Emails sent from one US location to a US person in another US location gets routed via Canada unbeknownst to the sender

- **Consider using encryption to mitigate risk**
Email Issues

- Emails with tech data are exports if they go to foreign location or go to a foreign national.

- If you do not know where the recipient is located, you do not know if it is an export. That does not mean it was not an export—it just means you didn’t know it was an export.

  *Example:* You send an email to your local co-worker who works in your facility but you did not know he is in China today.
Email Issues

- Consider developing a system for marking emails containing tech data and train employees not to access or decrypt emails with controlled tech data when they are in unauthorized locations.

- For more safety, develop a separate and secure email system that all employees must use to send emails containing tech data or proprietary information.
Email Recordkeeping Issues

- EAR and ITAR require that you keep all emails that contain tech data or software and all emails related to all exports
  - Work with IT to develop a system for this—many companies automatically delete all emails after a certain amount of time
  - One Option: cc: all export emails to a special address such as export@companyname.com. Then ask IT to not delete any emails for that account and give full administrative responsibility for that account to your export person.
  - Use email sniffer tool to detect and save all emails that contain tech data or software or that are related to exports
Mergers & Acquisition

- You have successor liability when you acquire a company that has violations
- You want to understand how your business will be integrated with the other company and determine what compliance steps and procedures will be necessary
Mergers & Acquisition

- Make US export/reexport compliance a standard element of your due diligence review prior to mergers & acquisitions

- May be similar to your internal self assessment:
  - What tech data do they possess, what it is jurisdiction and classification?
  - What are their methods of export/reexport and do they have compliance procedures for each method?
  - Look at sample of transactions/exports/reexport
Recent Changes to Tech Data Rules

- EAR License Exception STA
- ITAR Dual/Third Country National Retransfer Exemption
- Proposed Rules
License Exception STA

- Key element of Obama Administration’s Export Control Reform
- Implemented in June 16, 2011 Federal Register
- Could be one of the export authorizations for items moved from the USML to the Commerce Control List, if that happens
STA has two groups of countries.

STA Country Club 1 EAR 740.20(c)(1): Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, or the United Kingdom.

STA Country Club 2 EAR 740.20(c)(2): Albania, Hong Kong, India, Israel, Malta, Singapore, South Africa, or Taiwan.

STA Eligible Items 740.20(b)(2): STA may not be used for:

License requirements imposed by EAR Part 744 or 746

Items controlled for any of these reasons: encryption items (EI), short supply (SS), surreptitious listening (SL), missile technology (MT) or chemical weapons (CW)

Items in these ECCNs: 0A981, 0A982, 0A983, 0A985, 0E982, 1C351, 1C352, 1C353, 1C354, 1C360, 1E001, 1E351, 9A001, 9B001, 9D001, 9D002, 9D004, 9E001, 9E002, 9E003. Certain ECCNs are only partially excluded from STA—check 740.20(b)(2) for the details.

For more information go to: http://learnexportcompliance.bluekeyblogs.com/2011/07/13/export-control-reform-is-happening-now-bis-adds-license-exception-sta-to-ear/
For STA Country Club 1, paragraph 740.20(c)(1) says the items have to be controlled for one or more of these reasons, but not for any other reasons:

- national security (NS);
- chemical or biological weapons (CB);
- nuclear nonproliferation (NP);
- regional stability (RS);
- crime control (CC), or
- significant items (SI).

For STA Country Club 2, paragraph 740.20(c)(2) says eligible items are those that are both:

1) Controlled only for national security (NS) reasons; and

2) Not described in an STA paragraph in the ECCN for the item. The STA paragraphs in ECCNs tell you which items are not STA eligible for Country Club 2.

BIS wrote STA in a way that can be a bit confusing on this point. For the purpose of STA, either 1) ignore AT controls, or 2) remember that AT controls do not apply to any STA eligible countries so there really are not AT reasons of control.
The three steps of the paper trail are:

Step 1: The sending party (exporter, reexporter, or transferor within a country) gives the recipient the ECCN for each item being sent under STA. The sender only has to give the ECCN information for each item once, as long as that information remains accurate. So, if I tell you today that model 323 is ECCN 5A001 today, I don’t have to tell you on subsequent shipments.

Good news for recipients of my STA exports: The EAR says you can rely upon the ECCN classification I give you unless you know it is wrong.

Step 2: Prior to sending items, the sender gets an STA “Consignee Statement” from the recipient. The sender gets the “Consignee Statement” once and may use it to make multiple transfers as long as it continues to accurately describe the parties, items and ECCNs.

See 740.20(d)(2) for the text of the Consignee Statement.

The sender keeps a log of all STA shipments/transfers with a reference to the specific “Consignee Statement” used for each shipment/transfer.

Step 3: With every shipment/transfer the sender gives a written STA notice in paper or electronic form. The notice must identify which items in the shipment are moving under STA.

The License Exception STA paper trail must be established for every export, reexport and transfer under STA.

Paper trail requirements are in 740.20(d).

See 740.20(d)(4) for special information/paper trail for deemed exports and reexports.
May 16, 2011 Federal Register notice:
This exemption eliminates the requirement that foreign end-users and consignees authorized to receive items under TAAs and MLAs identify the nationalities of their dual/third country national employees in the agreement application and thereafter limit access to US defense articles to only approved nationalities. It also authorizes authorized end-users and consignees who received items under licenses or agreements to make retransfers to regular employees.

This exemption is available if the foreign party does 3 things:
1) Implement “effective procedures to prevent diversions destinations other than those authorized.” The effective procedures can be either of these:
   • A security clearance approved by the host nation government for its employees; or
   • The foreign party has a process in place to screen its employees and have signed non-disclosure agreements that provides assurances that the employee will not transfer any information to other persons unless authorized by the foreign party.

2) Screen its employees for substantive contacts with restricted or prohibited countries listed in 126.1 [e.g., China]. Substantive contacts include, but are not limited to, recent or regular travel to such countries, recent or continuing contact with agents and nationals of such countries, continued allegiance to such countries, or acts other indicating a risk of diversion.”

3) “Maintain a technology security/clearance plan that details its procedures for screening employees for such substantive contacts and maintain records of such screening. The technology security/clearance plan and screening records will be available to DDTC or its agents upon request.”

To see the Federal Register notice, go to http://www.pmddtc.state.gov/FR/2011/76FR28174.pdf
New ITAR 126.18 Exemption: Foreign Persons

- For agreements, there are now three options:
  - 124.16 NATO plus other favored country nationals
  - 126.18 Exemption
  - Name nationalities in the agreement

- It is possible to combine the options in an agreement, providing DDTC will approve the agreement
Proposed Definition of Defense Service

§ 120.9 Defense service. (a) The furnishing of assistance (including training) using other than public domain data to foreign persons ..., whether in the United States or abroad, in the design, development, engineering, manufacture, production, assembly, testing, intermediate or depot level repair or maintenance (see § 120.38 of this subchapter), modification, demilitarization, destruction, or processing of defense articles (see § 120.6 of this subchapter); or

(2) The furnishing of assistance to foreign persons, whether in the United States or abroad, for the integration of any item controlled on the [USML] or the Commerce Control List ... into an end item...or component... that is controlled as a defense article on the USML, regardless of the origin; or

(3) Training or providing advice to foreign units and forces, regular and irregular, regardless of whether technical data is transferred to a foreign person, including formal or informal instruction of foreign persons in the United States or abroad by any means including classroom or correspondence instruction, conduct or evaluation of training and training exercises, in the employment of defense articles; or

(4) Conducting direct combat operations for or providing intelligence services to a foreign person directly related to a defense article.

(b) The following is not a defense service:

(1) Training in the basic operation (functional level) or basic maintenance ... of a defense article; or

(2) Mere employment of a U.S. citizen by a foreign person; or

(3) Testing, repair, or maintenance of [an EAR item] that has been incorporated or installed into a defense article; or

(4) Providing law enforcement, physical security or personal protective training, advice, or services to or for a foreign person...using only public domain data; or

(5) Providing assistance (including training) in medical, logistical (other than maintenance), or other administrative support services to or for a foreign person.

Proposed 120.38 would define "organizational," "intermediate," and "depot" level maintenance.

Compliance: The Continuing Challenge

- It is impossible to have perfect compliance—don’t let the perfect be the enemy of the good.

- You have to determine the most effective way to use your limited compliance resources (time, money, people, IT, goodwill) to minimize as much risk as possible

- Compliance naturally:
  - Creates burdens
  - Adds costs
  - Prevents your organization from doing things the way it would like to do them
Compliance: The Continuing Challenge

- So, your challenge is to implement compliance procedures that
  - Create the least possible burden while ensuring the best possible compliance
  - Wisely allocate your resources
  - Involve program staff, sales, engineers, etc. in structuring compliance procedures
  - Regularly train all people directly or indirectly involved in exports/reexport
Compliance: The Continuing Challenge

- Find allies in your organization: top management, general counsel, security people, intellectual property people
- Demonstrate the risk of violations to top management and general counsel to support requirements for adequate resources
- Constantly assess your current state of compliance and identify places where you can make reasonable improvements—don’t bite off more than you can chew
Questions???

Please submit any questions you would like answered now in the Q&A section. We will do our best to answer all questions.

E-mail questions or comments on the content of this webinar to: John Black at jblack@tradecontrols.com

Upcoming Webinars
The Basics of India’s Export Controls: Expand Your Market and Stay in Compliance
February 27, 2013

EAR License Exceptions
March 13, 2013

Import 101 for All Business Professionals
March 21, 2013

Incotermes
April 10, 2013
Amber Road provides a single platform that plans and executes all aspects of global trade. By enabling companies to take a holistic, integrated approach to global trade, Amber Road accelerates the movement of goods across international borders, improves customer service and reduces global supply chain costs.

Amber Road includes deep functional capabilities across all areas of global trade – trade compliance, supply chain visibility, restricted party screening and origin management. Underpinning all of these solutions is Global Knowledge®, the most comprehensive, intelligent repository of global trade content available anywhere.
Compliance Simplified.

At MK Data Services we believe that compliance solutions should be easy-to-use, simple to access and cost effective. We offer a wide-array of import and export compliance solutions and services that are designed to help you achieve your compliance goals quickly and efficiently.

**Dynamic Screening**

In order to reduce risk and ensure the highest level of compliance you can leverage our dynamic screening solution. When a new entry is made in the denied parties list, your master list of customers will be screened and a report will be generated and automatically emailed to you. Our dynamic screening solution truly simplifies the process and enables you to focus on your business while ensuring compliance and reducing your risks.

**Bulk Screening**

Your time is valuable and screening your customers, vendors and trading partners takes time and effort. Take a load off and let us use our innovative software solution to quickly and efficiently screen for you. We will screen your list(s) against the most comprehensive lists of denied and restricted parties database available and provide you with a detailed report that outlines any potential risks that were identified, saving you time, money and ensuring your compliance with federal and international rules and regulations.

**MKDenial.com**

Our industry-leading Web-based offering is user-friendly and provides you with access to one of the most comprehensive databases of denied and restricted parties available. MKDenial.com was developed with U.S. exporters, financial institutions and freight forwarders in mind and we are consistently updating the site based on feedback from our more than 850 customers around the globe.
ERP Integration

By leveraging our Web Service Methods you can dynamically screen vendor, customer and trading partners against restricted or denied parties. Our team of talented developers has thoroughly documented everything required to access our Web Services. If desired or required we can provide support to your IT or development team to help ensure a smooth deployment of services.

MK Data Services is the preferred content provider for SAP Global Trade Management (SAP GTM), one of the world’s leading cross-industry trading solutions. With that said, we have integrated our Web Services with a wide range of ERP platforms including Oracle, JD Edwards, Sage, Microsoft and AS/400 based solutions.

Product Classifier

Classifying a product for export can be a time-consuming, labor intensive and tedious process. With that said it is a vital step in ensuring that your company is in compliance with U.S. export control regulations. Our product classifier solution will enable you to promptly and proficiently determine the proper ECCN for your product. It is an extremely valuable learning tool with links to the specific regulation citations so that you can classify your product with confidence.

Trade Content

We know how time consuming it can be to keep up with changes in the global trade environment, which is why we offer access to the following Harmonized Tariff Schedules (HTS):

- 101 Countries and multiple languages available
- Regular updates
- Duty and Tax Data
- Customized Content Based on Requirements
- NAFTA Rules of Origin

Would you like to learn more?

We offer many more tailor-fit services and solutions, if you would like to learn more about what we offer give us a call at 410-992-3282 or visit our website to learn more about how we can simplify compliance for you.

WWW.MKDATASERVICES.COM