Export Controls and Cloud Computing: Complying with ITAR, EAR and Sanctions Laws

WEDNESDAY, APRIL 23, 2014

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today’s faculty features:

Hilary L. Hageman, Vice President & Deputy General Counsel, CACI International, Arlington, Va.

Thaddeus R. McBride, Partner, Sheppard Mullin Richter & Hampton, Washington, D.C.

Laura Tomarchio, Director, Trade Compliance, Symantec, Mountain View, Calif.

Martina de la Torre, Sr. Manager, Global Trade Compliance, Symantec, Mountain View, Calif.

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
Tips for Optimal Quality

Sound Quality
If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial 1-888-601-3873 and enter your PIN when prompted. Otherwise, please send us a chat or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality
To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.
Continuing Education Credits

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

• In the chat box, type (1) your company name and (2) the number of attendees at your location
• Click the word balloon button to send
Agenda

• Introduction
• Cloud Computing and Export Controls
• Cybersecurity Developments and Cloud Export Compliance
• Compliance Challenges / Best Practices
Overview
Cloud Computing and Export Controls
What is Cloud Computing?

• 4 basic types
  ▫ **Public**: Provided by service provider to general public
  ▫ **Community**: Shared by organizations from a specific community
  ▫ **Private**: Provided for a single organization, hosted / managed internally or externally
  ▫ **Hybrid**: Combined deployment of one or more types
Increasing Cloud Usage

• U.S. government budget cutting and cost reduction initiatives

• U.S. government “Cloud First” policy

• Cost-savings and efficiencies driven by market
Export Controls

- Export controls apply to the export, sharing or transfer of **software** and/or **technology** (technical information) for the **development, production or use** of export controlled items.

- **Intangible transfers** of controlled software and technology via electronic means may require an export authorization.
Types of Technology

• Development Technology
  ▫ Related to all phases prior to serial production
  ▫ *e.g.*, design, assembly and testing of prototypes, pilot production schemes, process of transforming design data into a product

• Production Technology
  ▫ Related to all production phases
  ▫ *e.g.*, construction, production engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance

• Use technology
  ▫ Operation, installation (including on-site installation), maintenance (checking), repair, overhaul, and refurbishing
Examples of Exports

• Storing controlled technology / data on cloud servers located in China
• Encrypted email containing ITAR-controlled data routed through server in Calcutta
• U.S. project hosted by defense contractor on cloud allowing access by non-U.S. employees
• Hosting and using clouds without observing requisite IT security standard of care
Regulatory Guidance

- Department of Commerce has published two Advisory Opinions
  - Focus on responsibilities for cloud service providers
  - The Opinions do not specifically address responsibilities of cloud service users
<table>
<thead>
<tr>
<th>Guidance</th>
<th>Key Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advisory Opinion of 13 Jan 2009</td>
<td>• Cloud provider not considered “exporter” when user exports data on the cloud</td>
</tr>
<tr>
<td></td>
<td>• Provision of computational capacity not subject to EAR, but software provided to enable use may be subject to the EAR</td>
</tr>
<tr>
<td></td>
<td>• Cloud providers remain subject to restrictions on knowingly supporting WMD / missile-related activities</td>
</tr>
<tr>
<td></td>
<td>• Prohibition on access to computers / software under License Exception APP by nationals of Cuba, Iran, North Korea, Sudan and Syria does not apply if individual system access cannot be distinguished in the cloud</td>
</tr>
<tr>
<td></td>
<td>• Cloud providers not required to inquire about nationality of users</td>
</tr>
<tr>
<td>Guidance</td>
<td>Key Point</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Advisory Opinion of 11 January 2011</td>
<td>• Cloud providers not required to obtain “deemed export” licenses for non-U.S. IT administrators servicing / maintaining cloud computing systems</td>
</tr>
</tbody>
</table>
Perilous ITAR Landscape

• Cloud not specifically addressed in law and regulations
• No official guidance from DDTC
  ▫ No distinction between users and providers
  ▫ Strict liability
  ▫ Adherence to traditional rules
• Rapidly evolving IT security “standard[s] of care” enhance ambiguities
DTAG White Paper

- May 2013 White Paper from Defense Trade Advisory Group (DTAG)
  - Addresses issues posed by / possible solutions to issue of “exporting” data to a number of different servers for storage purposes
  - Proposed solution: encryption of materials stored in a cloud through a cipher text
  - Per DTAG, this is not an “export” unless the encrypted text and encryption key allowing text to be viewed in legible format were sent outside United States
Very practical guidance but ...

... no indication DDTC intends to accept these suggestions
Economic Sanctions

• Approximately 25 different U.S. sanctions regulations

• Regulator: U.S. Treasury Department, Office of Foreign Assets Control (OFAC)

• Jurisdiction over all U.S. persons
  • Includes all persons in United States
  • In case of Cuba and Iran, includes non-U.S. entities owned / controlled by a U.S. person
Sanctions - Types

- **Comprehensive**
  - Cuba, Iran, [North Korea], Sudan, Syria

- **Selective**
  - Belarus, **Russia**, Myanmar (Burma), Zimbabwe

- **Programmatic**
  - Narcotics Traffickers, Terrorists, Weapons Proliferators
Export of Services

• Prohibition on direct and indirect provision of services to sanctions targets

• Providing service **anywhere** may be prohibited if benefit of service is received by sanctioned party or in sanctioned country

  ▪ For example:

    • providing cloud computing services to a Syrian national SDN resident in London

    • repairing a private cloud server used by the national government of Belarus
Facilitation

- U.S. persons are prohibited from facilitating action that would be prohibited if performed by a U.S. person

- Broadly defined – covers virtually any assistance of a prohibited transaction

- *Example*: Cannot facilitate technology transfers for a non-U.S. company related to its business in Iran
Liability

IMPORTANT POINT:

There can be liability for any person, regardless of nationality, who causes a violation.
Recent Cybersecurity Developments and Cloud Export Compliance
Recent U.S. Cybersecurity Efforts

- DoD / GSA Joint Working Group on Improving Cybersecurity and Resilience through Acquisition

- Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011–D039)

- NIST Framework for Improving Critical Infrastructure Cybersecurity
DoD & GSA Working Group

Final Report of the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition

- Released January 23, 2014 by GSA and DoD
- Specific acquisition strategy recommendations
DFARS

- Unclassified **Controlled** Technical Information and Cyber Incident Reporting
  - Wide-ranging changes to DoD Contracts & Subcontracts
  - Requires government contractors to “provide adequate security” for technology systems “that *may* have unclassified controlled technical information [UCTI] resident on or transiting through...” (48 C.F.R. §§ 252.204-7012(b)(1))
  - Likely applicable to a contractor’s **entire** network
Controlled Technical Information

- *Controlled technical information* “means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.”

(48 C.F.R. § 252.204-7301)
DFARS (cont’d)

• Contractors required to report “cyber incidents” promptly to DoD
  ▫ Including the “possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information resident on or transiting through Contractor’s, or its subcontractors’, unclassified information systems.” (48 C.F.R. §§ 252.204-70)

• Requirements should be identified in specific clause in every DoD solicitation and/or contract
  ▫ Includes commercial items
  ▫ Clause will be required to be passed down to subcontractors
NIST Framework

• Framework For Improving Critical Infrastructure, Version 1.0
  ▫ Issued on February 12, 2014
  ▫ Developed in accordance with Executive Order 13636, “Improving Critical Infrastructure Cybersecurity"
  ▫ EO Directed NIST to collaborate with industry to develop a voluntary, risk-based cybersecurity framework
  ▫ Needs to be “prioritized, flexible, repeatable, performance-based and cost-effective.”
NIST Framework (cont’d)

• Applicable to “critical infrastructure” or “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof.” For example:

  • Power and utilities
  • Financial services
  • Telecommunications
  • Chemicals
  • Food and agriculture
  • Healthcare
NIST Framework (cont’d)

• Main elements
  ▫ **Framework core**: Includes suggestions on how to identify, protect, detect, and respond to cyber attacks
  ▫ **Tiers**: the levels of rigor for which organizations implement cybersecurity measures to identify where they fit in the four-tier structure; assesses moving to a more rigorous model (e.g., from localized to company-wide policies)
  ▫ **Profiles**: Identify what programs a company has implemented (“Current Profile”) and what is needed to meet additional risk management goals (“Target Profile”)

• Adoption is voluntary but encouraged
NIST Potential Benefits

- *Flexible* tools – it does not prescribe what to do or what tools to buy
- Federal programs may encourage participation:
  - cybersecurity insurance
  - grants
  - process preference
  - liability limitations
  - rate recovery for price regulated industries
  - influence on government sponsored cybersecurity research
NIST Benefits (cont’d)

• Over 3,000 individuals and organizations contributed to framework
• Comprehensive approach may mean:
  ▫ adoption may affect business relations with customers, contractors, and subcontractors
  ▫ may become *de facto* standard for private sector cybersecurity in data breach litigation
  ▫ could form basis for future legislation
Compliance Challenges and Best Practices
Challenges

- Seamless, real time, data exchange (and computing collaboration)
- May have countless contributors and recipients

**Special challenges:**
- Where is the data, really?
  - Data Privacy / Safe Harbor considerations
- Who has access?
  - Restricted / Denied Party Screening
  - End Users located in embargoed countries
- What is the end use?
Data Exchange Challenges (cont’d)

• Rapid adoption & changing faces
  ▫ Grids, team rooms, databases, connection spaces, SaaS, SaaP, Storage, etc.

• Company may be both a “provider” and “user” which creates internal users & external users

• Ingestion and extraction of data
  ▫ What is the data?
  ▫ Physical export or import of customer data
Export Authorization Challenges

• Export authorization for and product classification of the customer-facing cloud service and server-side code

• **Special challenge:**
  ▫ What is actually delivered to the customer?
    • Segregate code delivered to customer from server-side code
    • Classify the Cloud Service only
    • Classify the Cloud Service + client-side downloads
Export Challenges (cont’d)

• What code resides on the servers managed by the cloud service provider, and where?
  ▫ Classify the code that resides on the cloud servers
  ▫ Determine if servers sit only in the US or outside the US
  ▫ Obtain authorizations for development on server-side code
Challenges - Other Jurisdictions

- Export and Import Authorizations for other countries

- **Special challenges:**
  - Canada
  - EU
  - France
  - Israel
  - China
  - Russia
  - Japan
  - Other
Compliance Strategies

• Two basic approaches

1. Control access
   • If ITAR-controlled, limit to U.S. persons
     • Require servers and admin support to be in the U.S.
       ▪ Ensure screening for denied parties
   • If EAR controlled, limit to company employees
     • Leasing space / company
Compliance Approaches (cont’d)

2. Control data
   ▫ Limit to data in the public domain (or potentially NLR)
   ▫ Do not provide software for download
Strategies (cont’d)

• “Traditional” compliance measures, including:
  ▫ Clear classification of data in cloud zones
    • EAR – ECCN as needed
    • ITAR – simple ITAR designation likely enough
  ▫ Incorporate cloud into policies and training
    • Examples: Provisioning, APIs, usage policies
Traditional Compliance (cont’d)

• Ensure agreements for cloud use address risks
  • Server locations
  • U.S. person administrators if data is restricted
  • Type of content / data

• Ensure appropriately scoped licenses or other authorizations are in place
  • Terms and conditions to terminate services if export violation identified

• Training!
Strategies (cont’d)

• “Non-traditional” measures, including:
  ▫ Continually review evolving IT security legal and regulatory requirements for defense contractors
  ▫ Ensure ongoing monitoring of IT security technology threats/incidents—adapt accordingly
  ▫ Understand whether cybersecurity risks, incidents, and reporting have export control implications
Compliance Best Practices

• Risk Assessment

• Policies and Procedures

• Transaction / Business Activity Monitoring, Screening, Surveillance
Best Practices (cont’d)

• **Robust contract terms**
  ▫ Use to implement the compliance approach (access controls or limits on controlled technology)
  ▫ **End-use / end-user restrictions**
    • Prohibited content such as pornography
  ▫ **Delineate responsibilities of each party**
    • Include responsibilities of provisioning partners and end-user responsibilities
Best Practices (cont’d)

• Training

• Advice and Counsel

• Program Change Management

• Independent Testing / Audit

• Keep Good Records
Questions?
THANK YOU!

Laura Tomarchio
Symantec
Laura_Tomarchio@symantec.com

Thad McBride
Sheppard Mullin
tmcbride@smrh.com

Martina de la Torre
Symantec
Martina_delatorre@symantec.com

Hilary Hageman
CACI
hhageman@caci.com