HARVARD UNIVERSITY

| | |
|---|---|
| Guidance Title: | Export Control Guidance for Outsourcing Information Technology Services |
| Responsible Office: | OVPR |

# Export Control Guidance Document for Outsourcing Information Technology Services (1/22/2014)

## I. Introduction

The outsourcing of information technology (IT) services, while potentially beneficial for the management of research data, may also invite potential regulatory issues under the Export Control (EC) regulatory regime. The purpose of this Guidance Document is to provide an overview of critical EC issues related to obtaining IT services from sources outside of Harvard University.

## II. Application of Export Regulations to Information Technology

The federal Export Control regulations are a complex set of laws and regulations administered by the U.S. Department of State, the U.S. Department of Commerce, and the U.S. Department of Treasury that has established because of national security, economic interests, or foreign policy concerns. The State Department administers regulations that govern the export, re-export and import of both classified and unclassified defense-related articles, software, defense services, and related technical data from the United States abroad and/or to any foreign person, whether located in the United States or abroad. The U.S. Department of Commerce regulates the exports and re-exports of commercial and dual-use items (i.e., items that may have a military *or* civilian application), technology and software. The Department of Commerce regulations differ from the Department of State regulations in that the need for a license from the Commerce Department depends not only on the type of product but also on its final destination, the person who will receive it, and in some cases the end use of the item. The Treasury Department Office of Foreign Assets Control[1] (OFAC) administers embargos and sanctions that prohibit transactions with certain countries, entities, organizations, or individuals. The outsourcing of IT may raise issues under each of these regulatory regimes.

In general, it is safe to assume that if an item or technology is subject to export control, the data related to the item or technology is also subject to export control. Therefore, it is important to be cognizant of the Export Control implications of outsourcing information technology (IT) services including software development and information hosting services. Outsourcing activities that may trigger EC regulation include:

- The transfer of certain encryption software overseas;
- Software application development where a foreign national may have access to the applications; and
- Information storage using “Cloud Computing” where data subject to the EC regulations are stored in servers hosted overseas.

[1] For details on OFAC see: http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

## III. Guidelines for Outsourcing

### *a. Sanction and Embargos*

Sanctions and embargos are a set of targeted, or total, prohibitions against conducting business and trade with certain countries, individuals, and entities regardless of whether or not the technology is controlled by EC regulations. Depending of the type of the prohibitions, an export license, or authorization, from the U.S. government may be required. In order to determine if there are any sanctions or embargos that affect an IT outsourcing project:

i. Screen all individuals and entities involved in the provision of IT service against various lists covered under OFAC prohibitions before entering into an agreement with the entity or individual. Screening may be conducted through use of the Visual Compliance on-line platform or by referencing the blocked persons and country-specific sanctions lists found on the OFAC website.

   1. If the entity or individual is not on embargoed or sanctions lists, then proceed with determining if the items or technology is controlled pursuant to Commerce ("EAR") or State ("ITAR") regulations (see next Section).
   2. If the entity or individual appears on one of the lists, contact University Chief Research Compliance Officer (Ara_Tahmassian@Harvard.edu).

ii. Include provisions in the contract requiring that, prior to any change in the project personnel or sub-contractors, the contractor must notify Harvard University.

iii. New employees, or sub-contractors should be screened against the lists prior to approval of their engagement in the project.

*Note: The lists maintained by OFAC change regularly so it is important to be vigilant in conducting such reviews.*

### *b. Software Development*

If the contract for the development of a software application includes provisions for all, or portions of, the work to be conducted outside of the United States:

i. Determine if the technology (e.g. software code, encryption software and hardware containing encryption software, etc.) is subject to ITAR or EAR regulations. This can be achieved by checking the Commerce Control List (CCL) under EAR and the ITAR list to determine if the technology is covered. The CCL can be found at the **Commerce Control List** website; the ITAR Munitions List can be found at **ITAR Munitions List** website.

ii. If the technology is on the lists, determine the reason for control. The reason for control is listed at the beginning of the section that includes the technology.

iii. Identify the country where the work will take place, and determine if the controlled technology is permitted to be exported to that country without a license. The country chart can be found at the following link: [insert country chart]. If there is an "X" in the column for the relevant "reason for control," then you may need a license to outsource the proposed project.

iv. If the technology appears on the CCL or ITAR lists and the technology is controlled for export to the country where the work will take place, University Chief Research Compliance Officer can assist you in confirming that a license is required and securing a license to permit the work.

v. If the technology does not appear on the list and the country where the work will take place is not under an embargo, then the work can be conducted without additional EC restrictions.

vi. Document the review process (e.g. lists checked, Classification number from CCL, etc.) for potential regulatory audits.

*c. Data Hosting and Cloud Computing*

The use of "cloud computing" for "data hosting" provides a number of advantages. Included among these are reduced capital costs associated with infrastructure and broad access to the information across research groups and institutions. The use of cloud computing, however, like the outsourcing of IT services generally, may raise potential EC compliance issues. A Brooking Institute[2] report described the problem as: "*there is an inherent tension between cloud computing and export control. While the concept of the cloud is centered on the premise of removing the need to track the details of data movement among various destinations, export control regulations are built largely around restrictions tied to those very movements.*"

The Bureau of Industry and Security (BIS) issued an Advisory Letter on January 13, 2009[3] stating that:

> *[I]f the service provider ships or transmits software that is subject to the EAR, an "export" would occur. Similarly, if the service provider ships or transmits technology in the form of technical data (i.e., manuals, instructions, plans, etc.) or technical assistance (i.e., instructions, consulting services, etc.) that is not publicly available in order to give the user knowledge on how to access and use the computational capacity provided by grid or cloud computing, then that technology would be subject to the EAR*".

A follow-up BIS[4] Advisory Letter on January 11, 2011 indicated that *deemed export restrictions* (i.e. access to EC controlled data in the U.S. by foreign nationals) apply to any EC controlled information stored in "cloud computing."

**Pursuant to the University guidelines for Retention and Maintenance of Research Data, research records and data normally should be maintained in electronic computing systems maintained by the University.[5] Based on the complications associated with the identification of the location of the servers and the individuals who may have access to the EC controlled data, Harvard University stores such data only in servers owned by Harvard University and controlled by Harvard University employees who meet the regulatory requirements for such access.**

**For additional information or assistance in determining whether a license is required for software development projects or use of cloud computing, please contact University Chief Research Compliance Officer (Ara_Tahmassian@Harvard.edu)**

[3] See: BIS Advisory on Application of EAR to Grid and Cloud Computing Services 1/13/09. http://www.bis.doc.gov/index.php/policy-guidance/advisory-opinions

[4] See: BIS Advisory on Application of EAR to Grid and Cloud Computing Services 1/11/11. http://www.bis.doc.gov/index.php/policy-guidance/advisory-opinions

[5] See University guidelines entitled Retention and Maintenance of Research Records and Data: Principles and Frequently Asked Questions ("FAQs"). As stated in the guidelines, researchers should use Harvard electronic systems to store and transmit Research Records whenever possible, and must migrate Research Records to Harvard systems when capacity becomes available. When it is not possible to use Harvard systems due to a lack of internal capacity, researchers should only use external data storage providers that have been approved by the University CIO. This is especially important in the case of research involving EC-controlled information, because external data storage providers may lack adequate security measures.