HARVARD UNIVERSITY

Office of the Vice Provost for Research

Guidance Title:	Data Storage and Transmission
Responsible Office:	OVPR
Date:	1/9/2014
Revision Date:	10/25/2018

Export Control Guidance: Data Storage and Transmission

I. Application of Export Regulations to Data and Information Technology

a. Controlled Data

Many items and technologies involved in research at Harvard, including some that are readily available in the U.S., are subject to export control regulations intended to support national security policies, including cybersecurity policies, prevent the proliferation of chemical or biological weapons and nuclear or missile capability, and avoid arming adversaries or supporting terrorism.

In general, it is safe to assume that if an item or technology is subject to export control regulations, 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 ("EC") implications of data storage and transmission.

b. Sanction and Embargoes

Sanctions and embargoes are a set of targeted, or total, prohibitions against conducting business and trade with certain countries, individuals and/or entities regardless of whether or not the technology, information, or data stored or transmitted is controlled by EC regulations. In order to determine if there are any sanctions or embargoes impacting data storage and transmission:

i. Consult with your School or Institute's Export Control Administrator to determine if the data is controlled.
ii. Screen all individuals and entities involved in the provision of IT service pursuant to the University's SDN Screening and Monitoring Guidance.

The following activities may trigger export controls:

- The transfer of certain encryption software overseas;
- Software application development where a foreign national may have access to the applications; and
- Transmitting or storing electronic data in a military-embargoed country or in the Russian Federation, or otherwise failing to meet certain export control related security standards.

II. 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. Without implementing certain security measures, however, the use of such technology for the transmission and storage of electronic data may constitute an export of that data.

Transmitting or storing electronic data that meets certain security standards[1], would **NOT** constitute an export of that data, provided that the technology or software is:

1. Unclassified
2. Secured using "**end-to-end encryption**"
3. Secured using cryptographic modules (hardware or software) compliant with federal requirements[2]; and
4. Not intentionally[3] stored in a **military-embargoed country** or in the Russian Federation.

The regulation defines "**end to end encryption**" as:

(i) Uninterrupted cryptographic protection between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary) and

(ii) The means of decryption are not provided to any third party.

Military embargoed countries include:

- Afghanistan
- Belarus
- Burma
- Central African Republic
- China
- Congo, the Democratic Republic of
- Cuba

[1] A user may delegate security to a third party provider, but must ensure that such provider meets carve out criteria outlined above.

[2] Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other equally or more effective cryptographic means.

[3] Temporary storage on Internet servers while in transit is not considered intentional storage. However, storage on PCs while in military embargoed countries is considered intentional—in such circumstances, another authorization (e.g. TMP) is required.

- Cyprus
- Eritrea
- Georgia
- Haiti
- Iran
- Iraq
- North Korea
- Lebanon
- Libya
- Somalia
- South Sudan
- Sudan
- Syria
- Venezuela
- Zimbabwe

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[4]. Based on the risk associated with export controlled data, you should contact your School or Institute Export Control Administrator or OVPR and local IT Security to ensure that the storage of export controlled data meets the requisite licensure and security requirements.

For additional information please contact OVPR: Melissa Lopes at melissa_lopes@harvard.edu or Ara Tahmassian, ara_tahmassian@harvard.edu

[4] 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.