Export Controls and Cloud Computing

Bureau of Industry and Security
U.S. Department of Commerce

Presented by:
Tracy L. Patts
Foreign Policy Division

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

BIS Guidance on Cloud Computing

- Three directly relevant, published, Advisory Opinions, 2009-2014
- Definitional changes published in June 3 FR notice, in effect as of September 1, including the "encryption carve-out."
- Encryption carve-out provisions were **not** included in ITAR bookend of definitional changes – to be published separately.

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

BIS Guidance on Cloud Computing

- Jan. 2009 - a cloud provider that provides access to computational capacity is not the exporter of data derived from the computations because they are not the principal party in interest.
- Jan. 2011 - if the cloud provider is not the exporter, the cloud provider is not making a "deemed export" if their foreign national network administrators access the data.
- Nov. 2014 - remotely using controlled software is not an export itself, unless there is a transfer

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

June 3 FR Notice on Definitions

- Opportunity to address the issue; relevant changes in multiple locations in the proposed language.
- The term "cloud" not used in regulatory text – changes affect cross-national data transmission and release to non-U.S. nationals.
- Primary citation in EAR is in a new section, §734.18, "Activities that are not exports, reexports, or transfers."
- Three basic requirements for the carve-out: "end-to-end" encryption, applicability of FIPS standards, and prohibition on storage in D:5/Russia

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

"End-to-End" Encryption

- Defined as *uninterrupted* cryptographic protection between and originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary).
- Definition is intended to be flexible enough to accommodate different technical approaches (e.g. IPSEC VPN, SSL VPN, etc.)
- Definition is not intended to preclude service provider involvement (i.e., security can be delegated to a third party).

"Boundary to Boundary"

- In the June 3 FR notice, definition of "end-to-end" was changed from "system to system" encryption (e.g., PGP) to "security boundary to security boundary."
- Reflects common industry practice and provides more flexibility.
- Allows necessary services to be performed within the security boundaries while meeting the objectives of the rule.
- Caveat: boundary must be in-country – data cannot cross a national border in the clear.

Storage Restrictions

- "Intentional" storage prohibited in D:5 and Russia.
- Temporary storage on Internet servers while in transit not considered intentional storage.
- Storage on PC's while in D:5 *is* considered "intentional"; in such circumstances, another authorization (e.g., TMP) is required.
- As a practical matter, cloud providers serving western customers (including those owned by the PRC) have not located their resources in these countries.

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

Keys and other Access Data

- Release of keys, passwords or other data (access information) with "knowledge" that such release or transfer will result in release of underlying technical data is a controlled event.
- An unauthorized release of access information would be a violation to the same extent as unauthorized release of underlying data.
- Keys and other access data are *not* considered "technical data," and can thus be managed independently.

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

Issues Related to Execution

- Decryption outside the U.S. does not, of itself, constitute an export or release.
- Storage in the clear (after decryption) outside the U.S. does not, of itself, constitute an export or release.
- When transmission is decrypted and re-encrypted, "end-to-end" no longer applies. Subsequent transmission is a separate, new transmission.
- A user may delegate security to a third party provider, but must ensure that such provider meets carve out criteria (e.g. encrypts between cloud resources).

Conclusion

- Changes are intended to provide maximum flexibility to providers and users.

- BIS will provide additional guidance as more fact patterns emerge and technology evolves.

THANK YOU

For further inquiries, please contact:

John Haberstock
Regional Export Control Officer
U.S. Consulate General Hong Kong & Macau
Tel: +852 2521-6515
Fax: +852 5429-5952
john.haberstock@trade.gov

U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY