Alliance for Network Security

August 3, 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

Re: Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32) Published in 80 Fed Reg 31505 on June 3, 2015

Dear Sir/Madam:

On June 3, 2015, the Commerce Department's Bureau of Industry and Security ("BIS") published a Proposed Rule in the Federal Register entitled Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32). See 80 Fed Reg 31505.

The Alliance for Network Security ("ANS") is an industry association comprised of Alcatel-Lucent, Cisco Systems, Inc., Data Direct Networks, Google Inc., Hewlett-Packard Company, Hitachi Data Systems Corp., Intel Corp., Juniper Networks, Inc., Microsoft Corp., Novell, Inc., Qualcomm Inc., Rockwell Automation, Inc. and Symantec Corporation. For over fifteen years, ANS has advised the United States and foreign governments with respect to export and import controls on cryptography. We appreciate this opportunity to provide comments with respect to export controls on definitions that are relevant to the use of cryptography under the Export Administration Regulations (EAR).

The ANS members welcome this opportunity to comment on the Proposed Rule. Our primary interest is in three provisions that, taken together, provide a "safe harbor" for the export of controlled software and technology when used in some "cloud computing" environments (e.g., cloud file storage), including the following provisions in Section 734.18:

- Paragraph (a)(4)(ii), which requires that technology or software be secured using "end-to-end encryption";

- Paragraph (a)(4)(iii), which requires that the technology or software be secured using cryptographic modules compliant with Federal Information Processing Standard 140-2 (FIPS 140-2) or "other similarly effective cryptographic means"; and

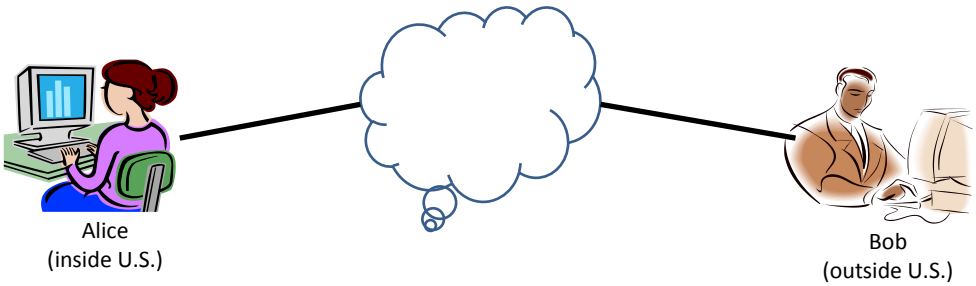
- Paragraph (b), which requires that the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

The Term "End-to-End" Should be Replaced with "Security Boundary or End Point-to-Security Boundary or End Point"

In Paragraph (a)(4)(ii) of Section 734.18, BIS establishes a requirement that information and software must be secured "end-to-end". We respectfully suggest that the term "end-to-end" should be replaced with "security boundary or end point-to-security boundary or end point".

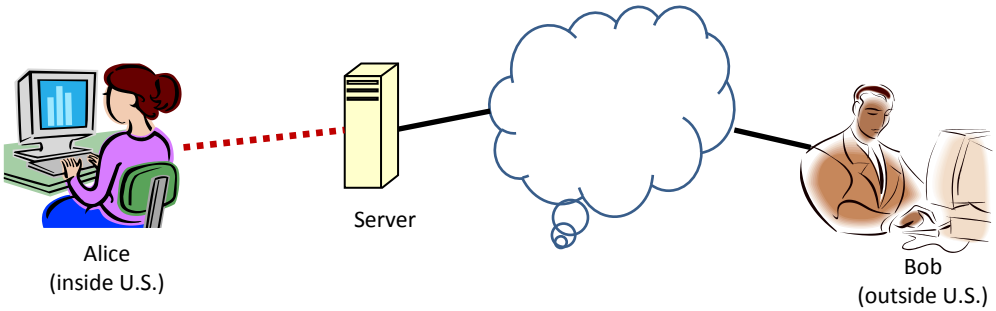
We understand from the preamble to the Proposed Rule that the "intent of this requirement is that relevant technology or software is encrypted by the originator and remain encrypted (and thus not readable) until it is decrypted by its intended recipient." This requirement is illustrated in Figure 1, where Alice, who is inside the United States, encrypts data on her personal computer or mobile device and sends it to the personal computer or mobile device of Bob, who is outside the United States:

Figure 1: End Point-to-End Point Encryption



However, consider also a second scenario, where Alice is a system administrator of a server which is located inside the United States, and authorizes a download of data to the personal computer or mobile device of Bob, who is outside the United States:

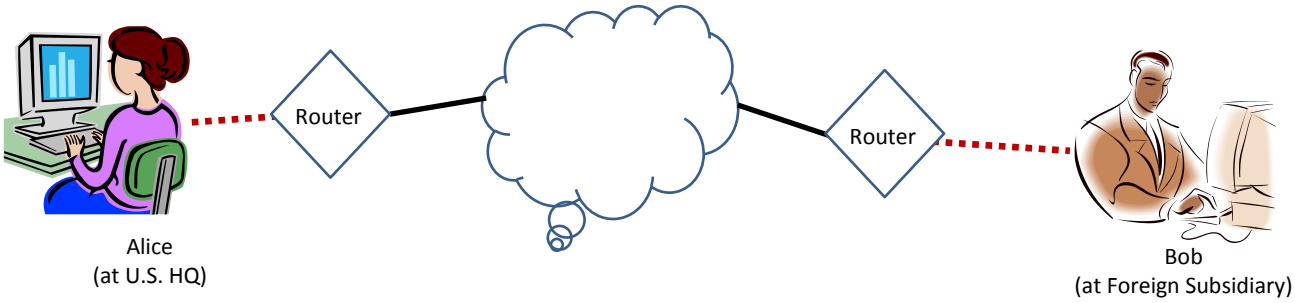
Figure 2: Security Boundary-to-End Point Encryption



Arguably, at the instant of export and until the moment of delivery, the data in transit is equally secure as the data in transit in Figure 1, even though the data in Figure 2 is not encrypted "end-to-end" as we understand that term. (We would refer to this as "security boundary-to-end point" encryption)

Please also consider a third scenario, where Alice is located at the headquarters of a company inside the United States, and Bob is located at the company's foreign subsidiary outside the United States. In this scenario, the data is encrypted by the edge routers at each office, and the data is sent in encrypted form through a virtual private network:

Figure 3: Security Boundary-to-Security Boundary Encryption



Arguably, at the time of export, the data in transit is equally secure as the data in transit in Figure 1, even though the data in Figure 3 is not encrypted "end-to-end" as we understand that term. Upon receipt, it is equally secure as any other technical data on Bob's computer or mobile device. The only time when the data is not secured is the brief moment, in transit, within the four walls of Bob's office. (We would refer to this as "security boundary-to-security boundary" encryption.) Please note that only the transfers of encrypted data data represented by black lines in these three figures would be exempt from the definition of "export". Transfers of plaintext represented by dotted red lines in figures 2 and 3 would not be exempt from the definition of "export".

We respectfully suggest that the term "end-to-end" should be replaced by "security boundary or end point-to-security boundary or end point" in the final rule.

The Term "Other Similarly Effective Cryptographic Means" Should Be Replaced with "Other Commercially Reasonable Cryptographic Means"

In Paragraph (a)(4)(iii) of Section 734.18, BIS establishes a requirement that the technology or software be:

> *Secured using cryptographic modules (hardware or software) compliant with 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 of Standards and Technology publications, or other similarly effective cryptographic means".

We respectfully suggest that the term "other similarly effective cryptographic means" should be replaced with "other commercially reasonable cryptographic means".

As a point of clarification, we think that the phrase "compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors" is not consistent with the terminology used in the Cryptographic Module Validation Program ("CMVP") for the FIPS 140 logo program. The CMVP validates cryptographic implementations of products according to the current version FIPS 140. The current version is FIPS 140-2. The CMVP Logo only has two options: "FIPS 140-2 Validated" and "FIPS 140-2 Inside". [1] FIPS 140-2 Validated means that the author of the cryptographic code paid for the validation of the cryptographic module. FIPS 140-2 Inside means that the author of the program is using a cryptographic module that was validated under CMVP by someone else. We think it would be preferable to use these terms in the final rule.

More importantly, in the experience of ANS member companies, a very small number of encrypted transmissions of technology and software actually take place using products that are either "FIPS 140-2 Validated" or "FIPS 140-2 Inside". The reasons include the facts that: (1) the FIPS algorithm selection [2]is very narrow, currently including AES, 3DES, ECC, some DH and others, but conspicuously omitting DES, RC2, RC4 and other algorithms in wide commercial use, (2) the FIPS process is voluntary, and can be expensive, and (3) FIPS products generally trail the "state of the art" by months or years, due to the time delays inherent in the FIPS process. An added complication is how ANS member companies and other U.S. Persons are supposed to determine whether a product that has *not* been through the FIPS process is "similarly effective"?

Therefore, we recommend that the term "other similarly effective cryptographic means" be replaced with "other commercially reasonable cryptographic means". By way of example, cryptographic means used to secure a company's valuable intellectual property could be used for purposes of meeting the requirement of Paragraph (a)(4)(iii) of Section 734.18.

If we revert to Figure 1, for example, this would authorize the use of PGP as one method of securing emails between Alice and Bob. If we revert to Figure 2, for example, this would authorize the use of implementations of the SSL/TLS protocol for client-server communications between Alice and

[1] http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPMM.pdf - see appendixes for details.
[2] http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPMM.pdf - page 44-45 a complete list is found here: http://csrc.nist.gov/groups/STM/cavp/validation.html - Included at end for reference.

Bob. If we revert to Figure 3, for example, this would authorize the use of implementations of the IPSec protocol for peer-to-peer communications between Alice and Bob.

Not Only the Sender and Recipient, but Any Third Party Who is a "U.S. Person" Should Be Permitted to Manage Keys or Other Means to Access Data in Unencrypted Form

In Paragraph (b) of Section 734.18, BIS establishes a requirement that the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

This requirement is particularly problematic to Internet service providers, application service providers and cloud service providers, who provide services to U.S. companies. For example, if a software as a service provider does not have access to encryption keys, functionality that requires data analytics such as search, indexing, anti-spam/anti-malware, configurable message transport rules, business intelligence, or issue replication for troubleshooting, may be degraded or rendered non-functional. We see no clear articulation of a rationale which would support exclusion of a business model involving outsourcing of security, including management of keys – provided of course that the Internet service provider, application service provider or cloud service provider itself is a U.S. Person.

Conclusion

We respectfully recommend that BIS make the following changes in the final rule:

- The Term "End-to-End" Should be Replaced with "Security Boundary or End Point-to-Security Boundary or End-Point";
- The Term "Other Similarly Effective Cryptographic Means" Should Be Replaced with "Other Commercially Reasonable Cryptographic Means"; and
- Not Only the Sender and Recipient, but Any Third Party Who is a "U.S. Person" Should Be Permitted to Manage Keys or Other Means to Access Data in Unencrypted Form.

Thank you for this opportunity to comment on the Proposed Rule in the Federal Register entitled Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32).

Sincerely,

Roszel C. Thomsen II