Perspecsys Inc.
1750 Tysons Blvd., Suite 1500
McLean, Virginia 22102

August 3, 2015

Ms. Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, DC 20230

Re: Response to Request for Comments Regarding Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32) – Use of Tokenization to Secure Technology in the Cloud

On June 3, 2015, the Bureau of Industry and Security (BIS) issued a Federal Register notice requesting comments on proposed amendments to the Export Administration Regulations (EAR, 15 C.F.R. Parts 730 – 774) that would revise certain definitions and update controls on the transmission and storage of technology in the cloud.[1]

PerspecSys Inc. (PerspecSys or the Company) respectfully submits these comments on the proposed definition of activities that are not exports, reexports or transfers (proposed § 734.18) and the revised subsection of license exception TMP regarding exports of technology to U.S. persons (§ 740.9(a)(3)).

In sum, PerspecSys supports amending the EAR to allow the secure transfer and storage of obfuscated technology in the cloud pursuant to the proposed § 734.18, but suggests that clarifying changes be made to §§ 734.18 and 740(a)(3) indicating that tokenization is an acceptable data obfuscation method in addition to encryption. According to many data security experts, tokenization provides data obfuscation, security, and operational functionality that is stronger than or as strong as encryption-only systems when implemented properly. Tokenization should therefore be explicitly recognized in the regulations as an approved data obfuscation method.

1. Company background

[1] Proposed Rule, Revisions to Definitions in the Export Administration Regulations, 80 Fed. Reg. 31505, 31517 (June 6, 2015).

PerspecSys provides cloud data control and security solutions to protect customers' sensitive information before it leaves their networks. In particular, PerspecSys' tokenization process allows customers to utilize cloud applications to process sensitive data without actually moving that sensitive data to the cloud. This process ensures data residency (e.g., that data remains on companies' secure network in the U.S.) and reliable obfuscation (e.g., there is no way to determine the clear text of the controlled data based on the information that is transmitted to the cloud).

2. Tokenization background

Tokenization is a process through which controlled or sensitive data or documents are obfuscated by replacing underlying clear text with a surrogate value called a "token." Tokens are used as reference or lookup values for underlying clear text or documents that are marked as sensitive by the data owner. Tokens are arbitrarily generated strings of characters with no mathematical or logical association to the clear text they replace or the documents they reference. PerspecSys tokens are generated and assigned through a sequentially generated and randomly assigned process (an important methodology distinction that will be discussed later in the request).

PerspecSys tokenization is used at the document and the field level.[2] Multiple tokens may be used for the same value depending on how narrowly or broadly a user sets "token spaces." Users of PerspecSys tokenization can define the scope of data that will share the same token for the same clear text data.[3] Users may also rotate token spaces over time so that a new set of tokens are assigned to data generated after a certain date.[4]

A "token vault" is a reference database containing a list of all tokens used and the corresponding clear text value. The token vault is maintained within the data owner's secured network and is encrypted for additional protection. PerspecSys's tokenization process occurs within a customer's secured network. Companies utilizing tokenization to protect EAR-controlled technology would treat the token vault as controlled and ensure that it is secured in compliance with EAR requirements (e.g., ensure that the token database is stored in an authorized country and secured from access by unauthorized persons).

Tokens are then transmitted to cloud providers for processing or storage.

---

[2] For example, a technical drawing would be replaced by a token value such as "prs_rky5433_z." That token would serve as a reference to the actual drawing (sometimes referred to as a "pointer token"), but would contain no information about the drawing. The token would then be transferred to the cloud, but the underlying drawing would remain locally stored within the data owner's secured network. Similarly, a unique field value in an enterprise resource planning (ERP) system (e.g. "John Smith" as the bill to party for a transaction) would be assigned an arbitrary token value such as "prs_AHJucx3_z." Again, the token value may be transmitted to the cloud, but the underlying "John Smith" value would not be transferred from the data owner's network. Data that is flagged as being non-controlled would pass through the system as clear text.

[3] For example, a user may specify a different token space be used for each field in an ERP system. As a result, "John Smith" as the "bill to" party may be represented by a token value of "prs_AHJucx3_z," while "John Smith" as the "ship to" party may be represented by a token value of "prs_KL3txL_2."

[4] As a result, "John Smith" as the "bill to" party may be represented in an ERP system by one token for a transaction on day 1, a second token on day 2, and a third token on day 3, and so on.

3. Security and data obfuscation advantages of tokenization

Tokenization, when implemented properly and at an appropriate security level as part of a comprehensive data security system,[5] provides distinct security advantages over data obfuscation methods based solely on encryption. Of course, not all forms of tokenization would be sufficient to properly secure technology in the cloud, just as not all forms of encryption are sufficient to secure data from unauthorized access. To secure controlled technology in the cloud, tokens must be non-authenticable and irreversible tokens.[6]

There is no way to mathematically "break" or derive the plain text of such strongly tokenized data without access to the token vault, which would be secured with other controlled data (or secured at an even higher level) within an encrypted database on a secured enterprise/agency datacenter in the United States. Furthermore, knowing the clear text or document associated with one or more tokens provides no insight to the clear text or document associated with any other token because tokens are not mathematically linked. In contrast, encrypted data stored on the cloud can be decrypted through the use of a key or through mathematical derivation (i.e., "breaking" the encryption). Furthermore, once the key to the encryption algorithm is obtained, all data encrypted using that algorithm may be decrypted. Failing to permit the use of tokenization to secure controlled technology would provide an unwarranted commercial advantage to one data security approach when an equivalent or superior technique provides the same or better security.

When tokenization is utilized, the underlying controlled technology would never be exported. The clear text of the underlying technology would be stored locally within the owner's secured network. The underlying data would never leave the owner's control in any format, either in clear text or in a mathematically derivable form. As a result, there can be no incidental export of the controlled technology, because only the replacement token value would be moved to the cloud (and potentially exported by cloud computing service providers).

---

[5] For example, such a system would include the following elements: (1) Controlled technology would be secured in the U.S. on servers restricted from foreign national access; (2) Tokens must be generated in such a way as to prevent any link between the clear text data and the token, including, for example, assignment of tokens through an index function or randomly generated number. A mathematically reversible cryptographic function would not be sufficient. (3) The entire tokenization system (including token generation, the tokenizing and de-tokenizing processes, token mapping, data vault and cryptographic management) should be housed in the U.S. and subject to security requirements at least as stringent as those applied to controlled technology (and likely far more restricted). PerspecSys secures the tokenization system using FIPS 140-2 encryption within an enterprise's or agency's secured network. (4) Additional best practices would include strong authentication and access controls, robust monitoring, and commination controls between the tokenized database and third party applications.

[6] See Tokenization Product Security Guidelines, PCI Security Standards Council, April 2015, p. 7, available at: https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf.

In addition, tokenization eliminates the need for complex key management procedures, which are costly to implement in a cloud environment and, if not properly controlled, are a potential security concern.[7]

4. Suggested revisions to the proposed Sec. 734.18(a)(4)

Given the potential advantages of using tokenization to secure controlled technology in the cloud, PerspecSys suggests that the proposed definition at § 120.52(a)(4) be modified to include tokenization as a permissible data security methodology. Specifically, PerspecSys suggests that the following changes be made to the proposed rule (bolded):

(a) * * *

(4) Sending, taking, or storing technology or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption **or tokenization**;

(iii) Secured using ~~**cryptographic**~~ **data obfuscation** 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 for Standards and Technology publications, or other similarly effective cryptographic means; and

(iv) Not stored in a country listed in Country Group D:5 (see Supplement No. 1 to part 740 of the EAR) or in the Russian Federation.

(b) Definitions. For purposes of this section, `end-to-end encryption **or tokenization'** means the provision of uninterrupted ~~**cryptographic**~~ **obfuscation** of data between an originator and an intended recipient, including between an individual and himself or herself. It involves ~~**encrypting**~~ **obfuscating** data by the originating party and keeping that data ~~**encrypted**~~ **obfuscated** except by the intended recipient, where the means to access the data in unencrypted **or clear text** form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

(c) The ability to access "technology" or "software" in ~~**encrypted**~~ **obfuscated** form that satisfies the criteria set forth in paragraph (a)(4) of this section does not constitute the release or export of such "technology" or "software."

---

[7] See SecaaS Implementation Guide, Category 8, Cloud Security Alliance, p. 18-19, available at: https://cloudsecurityalliance.org/download/secaas-category-8-encryption-implementation-guidance/.

These changes would allow industry to implement data security solutions incorporating tokenization methodologies that, when implemented properly, provide advantages over encryption-based data obfuscation systems.

5. Suggested revisions to clarify the amendment of Sec. 740.9(a)(3)

PerspecSys suggests that the proposed amendment to § 740.9(a)(3) be clarified to indicate that encryption and tokenization may be used to secure data pursuant to the exemption. As BIS is aware, tokenization and cryptography are distinct methods for obfuscating data. The current proposal lists encryption as an illustrative example of required security precautions, but does not reference tokenization, or more generally, data obfuscation. While the current language does not necessarily preclude the use of tokenization to comply with § 740.9(a)(3), it may create confusion among industry on which data security measures to adopt when securing controlled technology in the cloud.

As the BIS is aware, the Directorate of Defense Trade Controls (DDTC) issued an advisory opinion and related correspondence to PerspecSys indicating that tokenization may be used to secure ITAR-controlled technical data pursuant to the exemption in 2014.[8] The Company requests that the amended § 740.9(a)(3) include a similar reference to tokenization for the export of EAR-controlled technology to U.S. persons abroad.

Specifically, PerspecSys suggests that the following changes be made to the proposed rule (bolded):

> (a) * * *
>
> > (3) "Technology," regardless of media or format, may be exported by or to a U.S. person or a foreign national employee of a U.S. person, traveling or on temporary assignment abroad, subject to the following restrictions:
> >
> > > (i) Foreign nationals may only export or receive such "technology" as they are authorized to receive through a license, license exception other than TMP or because no license is required.
> > >
> > > (ii) "Technology" exported under this authorization may only be possessed or used by a U.S. person or authorized foreign national and sufficient security precautions must be taken to prevent the unauthorized release of the "technology." Such security precautions include **obfuscation (i.e., through** encryption **or tokenization)** of the "technology," the use of secure network connections, such as Virtual Private Networks, the use of passwords or other access restrictions on the electronic device or media on which the "technology" is stored, and the

[8] See DTC Case No. GC 0317-14 (Feb. 5, 2014) ("tokenization may be used to process controlled technical data using cloud computing applications without a license even if the cloud computing provider moved tokenized data to servers located outside the U.S., provided sufficient means are taken to ensure the technical data may only be received and used by" authorized persons).

use of firewalls and other network security measures to prevent unauthorized access.

(iii) The U.S. person is an employee of the U.S. Government or is directly employed by a U.S. person and not, e.g., by a foreign subsidiary.

(iv) Technology" authorized under this exception may not be used for foreign production purposes or for technical assistance unless authorized through a license or license exception other than TMP.

(v) The U.S. person employer of foreign nationals must document the use of this exception by foreign national employees, including the reason that the "technology" is needed by the foreign nationals for their temporary business activities abroad on behalf of the U.S. person.

6. Conclusion

PerspecSys appreciates BIS's and other agencies' consideration of our comments. Tokenization can offer reliable data obfuscation and data security sufficient to protect controlled technology in the cloud. We encourage the agency to revise the proposed amendments to specifically include tokenization as a valid data obfuscation methodology to encourage industry to adopt solutions that will best protect their data while it transits through overseas networks.

* * *

Please contact the undersigned at 703-712-4752 or gerry.grealish@Perspecsys.com with any questions or for additional information.

Sincerely,

Gerry Grealish
CMO, Perspecsys