DEPARTMENT OF STATE

22 CFR Part 120

[Public Notice: 10946]

RIN 1400-AE76

International Traffic in Arms Regulations: Creation of Definition of Activities That Are Not Exports, Reexports, Retransfers, or Temporary Imports; Creation of Definition of Access Information; Revisions to Definitions of Export, Reexport, Retransfer, Temporary Import, and Release

AGENCY: Department of State.

ACTION: Interim final rule; request for comment.

SUMMARY: The Department of State amends the International Traffic in Arms Regulations (ITAR) to create a definition of "activities that are not exports, reexports, retransfers, or temporary imports" by combining existing text from the regulations with new text regarding secured unclassified technical data. The activities included in the new definition are: launching items into space, providing technical data to U.S. persons within the United States or within a single country abroad, and moving a defense article between the states, possessions, and territories of the United States. The definition also clarifies that the electronic transmission and storage of properly secured unclassified technical data via foreign communications infrastructure does not constitute an export. Additionally, the Department amends the ITAR to create a definition of "access information" and revise the definition of "release" to address the provision of access information to an unauthorized foreign person.

DATES: *Effective date*: This interim final rule is effective on **[INSERT DATE 90 DAYS FROM DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

Comments due date: Interested parties may submit comments by **[INSERT DATE 30 DAYS FROM DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Interested parties may submit comments by one of the following methods:

• Email: DDTCPublicComments@state.gov with the subject line, "Revisions to Definitions; Data Transmission and Storage"

• Internet: At www.regulations.gov, search for this notice using Docket DOS–2019-0040.

FOR FURTHER INFORMATION CONTACT: Ms. Sarah Heidema, Director, Office of Defense Trade Controls Policy, Department of State, telephone (202) 663-1282; e-mail *DDTCPublicComments@state.gov*. ATTN: ITAR Amendment – Revisions to Definitions; Data Transmission and Storage.

SUPPLEMENTARY INFORMATION: The Directorate of Defense Trade Controls (DDTC), U.S. Department of State, administers the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130). The items subject to the jurisdiction of the ITAR, i.e., defense articles and defense services, are identified on the ITAR's U.S. Munitions List (USML) (22 CFR 121.1). With few exceptions, items not subject to the export control jurisdiction of the ITAR are subject to the jurisdiction of the Export Administration Regulations (EAR, 15 CFR parts 730 through 774, which includes the Commerce Control List (CCL) in Supplement No. 1 to part 774), administered by the Bureau of Industry and Security (BIS), U.S. Department of Commerce. Both the ITAR and the EAR create license requirements for exports and reexports of controlled items.

Items not subject to the ITAR or to the exclusive licensing jurisdiction of any other set of regulations are subject to the EAR.

On June 3, 2015, the Department of State published a proposed rule (80 FR 31525) (2015 proposed rule) and requested comments on an extensive array of proposed amendments to the ITAR, including the revision of key definitions, the creation of several new definitions, and the revision of related provisions. The proposed amendments also attempted to harmonize these definitions with the EAR to the extent appropriate. After reviewing the public comments on the 2015 proposed rule, the Department published an interim final rule on June 3, 2016 (81 FR 35611) (2016 interim final rule), which updated the definitions of "export" and "reexport or retransfer" and, in an effort to clarify and support the interpretation of these definitions, also created definitions of "release" and "retransfer." BIS concurrently published amendments (BIS companion rule) to definitions, including "export," "reexport," "release," and "transfer (in-country)" in the EAR (81 FR 35586). The Department subsequently reviewed the public comments on the 2016 interim final rule and published a final rule on September 8, 2016 (81 FR 62004) (2016 final rule), which revised the definition of "retransfer" and made other clarifying revisions. Not all of the amendments proposed in the 2015 proposed rule were adopted, and both the 2016 interim final rule and the 2016 final rule reserved the remaining amendments for consideration in separate rulemakings.

This interim final rulemaking addresses certain of the remaining amendments from the 2015 proposed rule, and the Department continues to reserve the remaining amendments for consideration in separate rulemakings. Included in this interim final rule is the creation of a definition for "activities that are not exports, reexports, retransfers, or

temporary imports" under a new ITAR § 120.54 (§ 120.52 in the 2015 proposed rule). Among other things, this provision provides that the properly secured (by end-to-end encryption) electronic transmission or storage of unclassified technical data via foreign communications infrastructure does not constitute an export, reexport, retransfer, or temporary import.

The Department recognizes the BIS companion rule addressed these issues with the creation of EAR § 734.18, and the Department has received repeated enquiries regarding when a similar rule would be issued regarding the ITAR. In an effort to align the definition in the ITAR with the definition in the EAR, the interim final rule described below is structured similarly to EAR § 734.18. The Department also recognizes that it has received public comments regarding these amendments to the ITAR. Where appropriate, those comments are addressed in the analysis below. In light of the potential impact the amendments in this rule may have on the regulated community's processes, and the updated security strength standards described below, the Department considered it appropriate to provide another opportunity for the public to submit comments and therefore publishes this rule as an interim final rule with the opportunity for the public to provide comment.

1. Definition of Activities that are not Exports, Reexports, Retransfers, or Temporary Imports

The Department adds § 120.54 to describe those "activities that are not exports, reexports, retransfers, or temporary imports" and do not require authorization from the Department. For the purpose of this preamble, the Department will use the term

"controlled event" to mean an export, reexport, retransfer, or temporary import, all of which require a DDTC license or other approval.

The first of five provisions in the new § 120.54 states in paragraph (a)(1) that it is not a controlled event to launch items into space. This activity is already excluded from the definition of an export in ITAR § 120.17(a)(6) and by statute, see 51 U.S.C. 50919(f). In an effort to consolidate the different activities that do not qualify as exports under the ITAR, this provision has been moved to § 120.54(a)(1), and the language has been simplified.

The second provision states in paragraph (a)(2) that it is not a controlled event to transmit or otherwise transfer technical data to a U.S. person within the United States from a person in the United States. In response to public comments, the updated version of paragraph (a)(2) provides that a transmission or other transfer between U.S. persons who are in the United States is unequivocally not a controlled event. However, any release to a foreign person remains a controlled event.

The third provision, which was not included in the 2015 proposed rule but is added here in response to public comments to that proposed rule, is found in the new paragraph (a)(3). This provision states that transmissions or other transfers of technical data between and among only U.S. persons in the same foreign country are similarly not reexports or retransfers so long as they do not result in a release to a foreign person or transfer to a person prohibited from receiving the technical data because that person is otherwise precluded from engaging in the regulated activity, for example a debarred person.

The fourth provision states in paragraph (a)(4) that it is not a controlled event to move a defense article between the states, possessions, and territories of the United States. One commenter requested that the Department revise paragraph (a)(4) to list explicitly the Virgin Islands of the United States, Guam, American Samoa, and the various United States Minor Outlying Islands. The Department will not make this change because the ITAR already defines the term "United States" in § 120.13, and that definition is applicable.

The fifth provision states in paragraph (a)(5) that it is not a controlled event to send, take, or store unclassified technical data when it is effectively encrypted using end-to-end encryption. Therefore, a controlled event does not occur when technical data is encrypted prior to leaving the sender's facilities and remains encrypted until decrypted by the intended authorized recipient or retrieved by the sender, as in the case of remote storage. The controlled event occurs upon the release of the technical data. If the technical data is decrypted by someone other than the sender, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, then the technical data is not secured using end-to-end encryption for purposes of paragraph (a)(5) and the original transmission was a controlled event.

The encryption must be accomplished in a manner that is certified by the U.S. National Institute for Standards and Technology (NIST) as compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2), or must meet or exceed a 128-bit security strength. At the time of publication of this rule, that criterion is expressed in "Table 2: Comparable strengths" of NIST Special Publication 800-57 Part 1, Revision 4. Additionally, the technical data may not be intentionally sent to a person in or

stored in a § 126.1 country or the Russian Federation, even in its encrypted state. This will allow for transmissions and storage of encrypted data in most foreign countries, so long as the technical data remains continuously encrypted while outside of the United States or until decrypted by an authorized intended recipient.

In response to public comments regarding the requirement of the 2015 proposed rule that the encryption be via a FIPS 140-2 compliant module, the Department added language that allows encryption through means other than FIPS 140-2 compliant modules, so long as it meets or exceeds a 128-bit security strength. One commenter suggested that the Department retain only FIPS 140-2 to encourage interoperability between systems, but the overwhelming number of commenters requested other encryption modules be allowed. The Department also clarified that intentional storage in the Russian Federation or a §126.1 country constitutes a controlled event. However, incidental collection by a foreign intelligence service or transient storage that is incidental to sending information via the Internet does not.

Further, in response to public comments, the Department revised paragraph (b) to clarify the definition of end-to-end encryption. The cryptographic protection must be applied prior to the data being sent outside of the originator's security boundary and remain undisturbed until it arrives within the security boundary of the intended recipient. For communications between individuals, this can be accomplished by encrypting the data on the sender's computer prior to emailing or otherwise sending it to the intended recipient. For large entities, the security boundary may be managed by IT staff, who will encrypt the data before it leaves the entity's secure network and decrypt it on the way into the network. However, in all instances, the means of decryption must not be provided to

any third party and the data must not have the cryptographic protection removed at any point in transit.

One commenter suggested that the Department define which modules under FIPS 140-2 are compliant and which NIST publications are applicable, in the rule. The Department disagrees with this comment. Compliance with any of the four levels set out in FIPS 140-2 is sufficient for the purposes of this section. Exporters are free to choose the level that best meets their needs. Different NIST publications are relevant to each standard, so the applicable publications will depend on the standard used.

One commenter suggested that the Department provide one year from the issuance of a new NIST standard for implementation. The Department disagrees with this comment. The NIST standards will be final and applicable when NIST makes them the standard.

One commenter requested that the Department allow a transition period so that exporters can implement IT systems compliant with paragraph (5). The Department disagrees with this comment. Paragraph (5) creates a mechanism for companies to send and store technical data outside the United States without engaging in a controlled event. Until companies implement an IT system that is compliant with paragraph (5), they may not take advantage of this paragraph, but nothing in paragraph (5) places any new requirements on exporters, therefore there is no need for a transition period.

One commenter suggested that the Department revise paragraph (b) to say "the means to access the data in unencrypted form is not 'released' to any third party" rather than "the means to access the data in unencrypted form is not given to any third party," as "release" is a defined term. The Department disagrees with this comment. The

Department did revise this concept in paragraph (b) to require that "the means of decryption are not provided to any third party," but the Department chose not to use the word "released" because that word has a technical definition that would not be applicable in this usage.

Several commenters requested that the Department provide a safe harbor, of sorts, by only requiring that cloud customers obtain contractual assurances that the data would not be stored in a § 126.1 country or the Russian Federation. The Department disagrees with this comment. Such a provision would not be in the national security or foreign policy interests of the United States. The Department recognizes it can be difficult to control the actions of third parties, including partners, service providers, and subcontractors, and will review potential violations on a case-by-case basis, subject to the totality of the facts and circumstances comprising the issue at hand.

One commenter requested that the Department clarify that appropriately encrypted transmissions may transit the Russian Federation or a § 126.1 country and still qualify for this provision. The Department clarified this point by adding the word "intentionally," to differentiate those electronic transmissions that were intentionally sent to Russia or a § 126.1 country, and those that simply transited them in route to another country. The commenter also provided an example of such a transmission where an email server is located in the Russian Federation or a § 126.1 country. Transmission through these destinations is allowed, including temporary storage incident to Internet transmissions, but long-term storage of the information, such as is commonly done on email servers, is prohibited in these destinations. Prior to using this provision, putative

exporters should ensure that the intended recipient or any intended remote storage provider does not store their information in the Russian Federation or a § 126.1 country.

One commenter requested that the Department provide that emails between authorized parties in the same country also be included in the definition of activities that are not exports, reexports, or retransfers if they happen to transit a third country, even if the technical data is not encrypted as described in paragraph (5). The Department notes that transmissions between U.S. persons in the United States are not exports under paragraph (2), but that with respect to transmissions in foreign countries, only those communications that remain in one country between only U.S. persons are excluded under paragraph (3). If a company in a foreign country is concerned that emails that include technical data may transit third countries, it should encrypt those communications consistent with paragraph (5).

Several commenters requested that the Department revise the local definition of end-to-end encryption to allow for information security mechanisms that render the data into clear text in route to the intended recipient, for processing via applications, such as anti-virus software or spell-check. The commenters also note that multiple layers of encryption may be applied and removed throughout the transit of the data. The Department disagrees with this comment. Use of paragraph (a)(5) requires that the technical data subject to the ITAR be continuously encrypted at all times while outside of an authorized security boundary. The Department is aware that there are many ways that this provision can be implemented; some of which would allow an entity to run anti-virus or other security scans prior to allowing the data onto its servers. As long as that initial encryption layer remains intact, the addition or removal of subsequent layers of

encryption, which may or may not meet the FIPS 140-2 standard, is not relevant to the application of this section.

One commenter requested that the Department include the electronic storage in the United States and transfer from the United States of non-U.S. origin technical data by non-U.S. persons within the activities that are not an export, reexport, or retransfer, even when not encrypted. The Department disagrees with this comment. Non-U.S. origin technical data transiting or stored in the United States that is encrypted in the manner described in paragraph (a)(5) (i.e., it remains encrypted at all times between originator and recipient, including at any time while in the United States), does not require authorization from the Department, unless it originates in or is sent to a country listed in § 126.1 or the Russian Federation.

One commenter stated that paragraph (a)(5) in this rule does not authorize the export of technical data in a physical medium and requested that the Department revise paragraph (a)(5) to allow the shipment or carriage of technical data in a physical medium that has been properly encrypted. The Department notes that the comment mischaracterizes the activity. The movement or storage of controlled technical data in a properly encrypted state outside of the United States is not an export as defined in § 120.17(a)(1), the specific concern raised by the commenter, or a controlled event of any type, and does not require authorization. The Department notes that paragraph (a)(5) is not limited to electronic transmissions and the shipment or carriage of technical data in a physical medium is not a controlled event, so long as all of the conditions are met.

One commenter requested that the Department expand paragraph (a)(5) to cover tokenization, as well as encryption. Tokenization is a process whereby individual

elements of a document, be they letters, words, diagrams, or pictures, are replaced by a representative token. As described by the commenter, the tokens are assigned randomly and a key of the document is created. The document may not be returned to the original text from the tokens without use of the specific key for that document. This process is different from encryption, in that encryption uses an algorithm to encode the document, such that representative characters are assigned according to a mathematical formula that can, at least theoretically, be deciphered through analysis of the encrypted text. The Department will not add tokenization. There is no NIST or other comparable standard that the Department can reference to set a minimum threshold for implementation of tokenization.

One commenter suggested that the Department encourage other jurisdictions to adopt a provision similar to paragraph (a)(5) in their export control systems. The Department agrees, and has already engaged in discussions with allies regarding paragraph (a)(5).

One commenter requested that the Department add shipping to and within the territory of an approved end-user as an activity that is not an export, reexport, or retransfer. The Department disagrees with this comment. A shipment to the territory of an approved end-user is an export or reexport that requires authorization. Shipments within the territory of an authorized end-user will likewise require authorization if the shipment is to someone other than the authorized end-user or for activities other than the authorized end-use.

One commenter requested that the Department create a definition of "basic technical data" and include the sharing of such information in this section, analogizing to

the sharing of the owner's manual for a car. The Department disagrees with this comment. The export of technical data requires authorization from the Department. If the Department were to define some portion of technical data that does not warrant control, the Department would revise § 120.6 or § 120.10 to exclude it.

One commenter suggested that the Department include shipments to military post offices in this section, noting that the National Industrial Security Program Operating Manual (NISPOM) treats transfers to military post offices as domestic transfers. The Department disagrees with this comment. The export of a defense article shipped to a military post office via the U.S. Postal Service is accomplished by the U.S. military and therefore may be authorized without a license via § 126.4 of the ITAR, so long as the other terms and conditions of that provision are met.

2. Revised Definitions of Export, Reexport, Retransfer, and Temporary Import

As stated above, the Department moves the language of § 120.17(a)(6), which articulates that it is not an export to launch items into space, to § 120.52(a)(1), and simplifies the language. In its place, the Department adds a new § 120.17(a)(6) in order to include within the definition of export the release through the use of access information of previously encrypted technical data as described in § 120.50(a)(3) (to a foreign person, no matter where located) and (a)(4) (causing the technical data to be in an unencrypted form out of the United States). The Department added a citation to § 120.54 to §§ 120.17(a), 120.18, 120.19(a), and 120.51(a), which define export, temporary import, reexport, and retransfer, respectively, to exclude from those definitions activities identified in § 120.54. In addition, the Department takes this opportunity to revise

§ 120.17(a) in order to mirror the construction of the other definitions of controlled activities and lead with the defined term of "export."

3. Definition of Access Information

The Department adds new § 120.55 to define "access information." Access information allows access to encrypted technical data in an unencrypted form, such as decryption keys, network access codes, and passwords. An authorization is required to release technical data through access information to the same extent that an authorization is required to export the technical data when it is unsecured by encryption.

Several commenters requested that the Department adopt the knowledge requirement that was included in the BIS companion rule and now appears in EAR § 734.19. The Department disagrees with this comment. As provided in §§ 120.50(b) and 120.54(b), an existing authorization for the release of technical data to the foreign person must be in place prior to the provision of access information to the foreign person that will allow the transition of the encrypted technical data to an unencrypted state.

4. Revised Definition of Release

The Department adds two new subparagraphs to paragraph (a) and a new paragraph (b) to the definition of release in § 120.50 in order to clarify what constitutes a release of technical data, a controlled event requiring authorization from the Department, and the provision of access information that may result in the release of technical data. Paragraph (a)(3) makes it a release of technical data to use access information to cause or enable a foreign person to access, view, or possess technical data in unencrypted form. Paragraph (a)(4) makes it a release of technical data to use access information in a foreign country to cause technical data to be in unencrypted form, including when such

actions are taken by U.S. persons abroad. Most U.S. persons will be authorized to release the technical data abroad to themselves or over their employer's virtual private network through the exemption at ITAR § 125.4(b)(9).

The 2015 proposed rule proposed a new paragraph (a)(5) to make it a release to provide access information to a foreign person that can cause or enable access, viewing, or possession of technical data in unencrypted form. It also proposed a Note to paragraph (a) in order to clarify the license requirement regarding technical data secured by the access information when a release occurs under the proposed paragraphs (a)(3), (a)(4), or (a)(5).

In a change from the 2015 proposed rule, the Department now includes at paragraph (b) language derived from the proposed paragraph (a)(5) and Note included in that draft. The new paragraph (b) clarifies that the provision of access information to a foreign person is not itself a controlled event; there is no need for an application by the access information provider, or for the Department to issue an authorization, for the provision of access information. However, in order for the Department to effectively control the release of technical data to a foreign person in certain circumstances, paragraph (b) requires an authorization for a release of technical data to a foreign person before providing the access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data. In the absence of an authorization for the release of technical data in such circumstances, the provision of access information to a foreign person is a violation of ITAR § 127.1(b)(1) for failure to abide by a rule or regulation contained in this subchapter.

Furthermore, causing or enabling a foreign person to access, view, or possess unencrypted technical data may constitute a separate violation of ITAR § 127.1(a), if the exporter (or reexporter or retransferrer) in question has not received prior authorization from the Department in the form of a license or other authorization (e.g., exemption). As stated in ITAR § 120.54(b), in order for the sending, taking, or storing technical data to meet the requirements of end-to-end encryption and therefore to constitute an activity that is not a controlled event under ITAR § 120.54(a)(5), the intended recipient must be the originator, a U.S. person in the United States, or otherwise authorized to receive the technical data in an unencrypted form.

The Department recognizes that the 2015 proposed rule contained draft language for a new § 127.1(b)(4) that would have listed the types of controlled events involving the secured unclassified technical data described in this interim final rule's § 120.54(a)(5). The Department did not receive any public comments on this proposed amendment. Nevertheless, once the Department decided to establish a new definition for "access information" in § 120.55 that is distinct from the definition of technical data in § 121.10, it seemed more appropriate to include descriptions of the relevant controlled events under the definition of release in § 120.50 because that provision was added to the ITAR in order to describe more effectively the controlled disclosure of information. Moreover, this construction is analogous to how the EAR defines the term "access information" in EAR § 772.1 and uses that term in § 734.19 to describe controlled events related to "activities that are not exports, reexports, or retransfers" under § 734.18.

Finally, the Department adds and reserves §§ 120.52 and 120.53.

Regulatory Analysis and Notices

Administrative Procedure Act

This rulemaking is exempt from section 553 (Rulemaking) and section 554 (Adjudications) of the Administrative Procedure Act (APA) pursuant to 5 U.S.C. 553(a)(1) as a military or foreign affairs function of the United States Government. Although the Department is of the opinion that this interim final rule is exempt from the rulemaking provisions of the APA, the Department published this rule as a proposed rule (80 FR 31525) with a 60-day provision for public comment, published an interim final rule (81 FR 35611) with a 30-day provision for public comment and three-month delayed effective date for certain provisions thereof, and now as another interim final rule with a 30-day provision for public comment and three-month delayed effective date for the provisions identified herein. Those publications were without prejudice to the Department's determination that controlling the import and export of defense services is a foreign affairs function.

Regulatory Flexibility Act

Since the Department is of the opinion that this rulemaking is exempt from the rulemaking provisions of 5 U.S.C. 553, there is no requirement for an analysis under the Regulatory Flexibility Act.

Unfunded Mandates Reform Act of 1995

This rulemaking does not involve a mandate that will result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any year and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996 (the "Act"), a major rule is a rule that the Administrator of the OMB Office of Information and Regulatory Affairs finds has resulted or is likely to result in: (1) An annual effect on the economy of $100,000,000 or more; (2) a major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions; or (3) significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and foreign markets.

The Department does not believe this rulemaking is a major rule within the meaning of the Act. The means of solving the issue of data protection are already both familiar to and extensively used by the affected public in protecting sensitive information.

Executive Orders 12372 and 13132

This rulemaking will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this rulemaking does not have sufficient federalism implications to require consultations or warrant the preparation of a federalism summary impact statement. The regulations implementing Executive Order 12372 regarding intergovernmental consultation on Federal programs and activities do not apply to this rulemaking.

Executive Orders 12866 and 13563

Executive Orders 12866 and 13563 direct agencies to assess costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributed impacts, and equity). The executive orders stress the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rulemaking has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the rulemaking has been reviewed by the Office of Management and Budget (OMB).

Executive Order 12988

The Department has reviewed the rulemaking in light of sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate ambiguity, minimize litigation, establish clear legal standards, and reduce burden.

Executive Order 13175

The Department has determined that this rulemaking will not have tribal implications, will not impose substantial direct compliance costs on Indian tribal governments, and will not preempt tribal law. Accordingly, Executive Order 13175 does not apply to this rulemaking.

Executive Order 13771

This final rule is not subject to the requirements of Executive Order 13771 because it is issued with respect to a military or foreign affairs function of the United States.

Paperwork Reduction Act

This rulemaking does not impose any new reporting or recordkeeping requirements subject to the Paperwork Reduction Act, 44 U.S.C. Chapter 35; however, the Department seeks public comment on any unforeseen potential for increased burden.

List of Subjects in 22 CFR 120

Arms and munitions, Classified information, Exports

Accordingly, for the reasons set forth above, title 22, chapter I, subchapter M, part 120 of the Code of Federal Regulations is amended as follows:

PART 120 – PURPOSE AND DEFINITIONS

1. The authority citation for part 120 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2794; 22 U.S.C. 2651a; Pub. L. 105–261, 112 Stat. 1920; Pub. L. 111–266; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

2. Section 120.17 is amended by revising paragraphs (a) introductory text and (a)(6) to read as follows:

§ 120.17 Export.

(a) *Export*, except as set forth in § 120.54, § 126.16, or § 126.17, means:

* * * * *

(6) The release of previously encrypted technical data as described in § 120.50(a)(3) and (4) of this subchapter.

* * * * *

3. Section 120.18 is revised to read as follows:

§ 120.18 Temporary import.

Temporary import, except as set forth in § 120.54, means bringing into the United States from a foreign country any defense article that is to be returned to the country from which it was shipped or taken, or any defense article that is in transit to another foreign destination. Temporary import includes withdrawal of a defense article from a customs bonded warehouse or foreign trade zone for the purpose of returning it to the country of origin or country from which it was shipped or for shipment to another foreign destination. Permanent imports are regulated by the Attorney General under the direction of the Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (*see* 27 CFR parts 447, 478, 479, and 555).

4. Section 120.19 is amended by revising paragraph (a) introductory text to read as follows:

§ 120.19 Reexport.

(a) *Reexport*, except as set forth in § 120.54, § 126.16, or § 126.17, means:

* * * * *

5. Section 120.50 is amended as follows:

a. By removing the word "or" at the end of paragraph (a)(1);

b. By removing the period and adding in its place a semi-colon at the end of paragraph (a)(2); and

c. By **a**dding paragraphs (a)(3) and (4) and (b).

The additions read as follows:

§ 120.50 Release.

(a) * * *

(3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or

(4) The use of access information to cause technical data outside of the United States to be in unencrypted form.

(b) Authorization for a release of technical data to a foreign person is required to provide access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data.

6. Section 120.51 is amended by revising paragraph (a) introductory text to read as follows:

§ 120.51 Retransfer.

(a) *Retransfer*, except as set forth in § 120.54, § 126.16, or § 126.17, means:

* * * * *

§ 120.52 [Reserved]

7. Add reserved § 120.52.

§ 120.53 [Reserved]

8. Add reserved § 120.53.

9. Section 120.54 is added to read as follows:

§ 120.54 Activities that are not exports, reexports, retransfers, or temporary imports.

(a) The following activities are not exports, reexports, retransfers, or temporary imports:

(1) Launching a spacecraft, launch vehicle, payload, or other item into space.

(2) Transmitting or otherwise transferring technical data to a U.S. person in the United States from a person in the United States.

(3) Transmitting or otherwise transferring within the same foreign country technical data between or among only U.S. persons, so long as the transmission or transfer does not result in a release to a foreign person or transfer to a person prohibited from receiving the technical data.

(4) Shipping, moving, or transferring defense articles between or among the United States as defined in § 120.13 of this subchapter.

(5) Sending, taking, or storing technical data that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with the 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 (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES-128);

(iv) Not intentionally sent to a person in or stored in a country proscribed in § 126.1 of this subchapter or the Russian Federation; and

NOTE TO PARAGRAPH (a)(5)(iv): Data in-transit via the Internet is not deemed to be stored.

(v) Not sent from a country proscribed in § 126.1 of this subchapter or the Russian Federation.

(b)(1) For purposes of this section, end-to-end encryption is defined as:

(i) The provision of cryptographic protection of data, such that the data is not in an unencrypted form, 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.

(2) The originator and the intended recipient may be the same person. The intended recipient must be the originator, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, such as by a license or other approval pursuant to this subchapter.

(c) The ability to access technical data in encrypted form that satisfies the criteria set forth in paragraph (a)(5) of this section does not constitute the release or export of such technical data.

9. Section 120.55 is added to read as follows:

§ 120.55 Access Information.

Access information is information that allows access to encrypted technical data subject to this subchapter in an unencrypted form. Examples include decryption keys, network access codes, and passwords.

Christopher A. Ford,

Assistant Secretary,

International Security and Nonproliferation,

U.S. Department of State.

Billing Code 4710-25

[FR Doc. 2019-27438 Filed: 12/23/2019 8:45 am; Publication Date: 12/26/2019]