August 3, 2015

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

Sent via email to: publiccomments@bis.doc.gov

Re: RIN 0694–AG32 - Revisions to Definitions in the Export Administration Regulations

Dear Sir/Madam:

Google welcomes the opportunity to comment on the proposed rule regarding the definition of various terms in the Export Administration Regulations ("EAR"). 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.) We provide comments on the following definitions.

Definition of "Peculiarly Responsible"

In the Federal Register notice of this proposed rule, BIS asked whether the proposed definition of ''peculiarly responsible'' effectively explains how items may be ''required'' for particular functions. It does not. The proposed definition reaches too far and would control too much information (i.e. "technology"). In particular, the "release" portion of the "catch and release" process laid out in the proposed definition will lead to too many absurd results. In the overwhelming majority of analyses, the illustration of technologies "A," "B," "C," "D," and "E" in the existing definition of "required" is sufficient to distinguish technologies that are peculiarly responsible (and thus controlled) from those that are not.

In the term "peculiarly responsible," it is significant that "responsible" is modified by the word "peculiarly," which denotes a special, causal relationship with the thing that is being controlled. The proposed definition of "peculiarly responsible" effectively removes "peculiarly" from the equation and controls a wider swath of "technology" than is warranted.

We will provide examples where the proposed definition of “peculiarly responsible” leads to odd and undesirable results. These examples are oversimplified to some degree, but they are intended to be simple for the sake of illustration and to avoid discussing any specific examples that could reveal Google confidential information. We also comment on the relationship between the proposed definition and the General Technology Note, and we offer recommendations regarding the proposed definition.

A. Example 1: Heat Sink Design “Technology”

Assume that a U.S. company called “Heats Inc.” produces heat sinks for a variety of computer manufacturers. Suppose that all but one of Heats Inc.’s customers make mass-market computers classified under ECCN 4A994, and they purchase Heats Inc.’s straight-fin heat sinks having a length and width of one inch. The 1” x 1” heat sink and its design “technology” would both be classified under EAR99. Say that Heats Inc.’s other customer, “HPC,” manufactures computers classified under ECCN 4A003.b and purchases straight-fin heat sinks with a length and width of two inches. Heats Inc. only sells 2” x 2” heat sinks to HPC, has no intent to sell or market them to other computer manufacturers, designed the larger heat sink at HPC’s specific request, and learned during the course of business discussions that HPC’s computers are classified under 4A003.b. Assume that Heats Inc. is the only heat sink manufacturer in the world producing straight-fin heat sinks measuring two inches by two inches. Further assume that the only difference in the design of the two types of heat sinks is in the length and width dimensions.

Now let us determine the ECCN of the design technology for the 2” by 2” heat sink using the “catch and release” process in the proposed definition of “peculiarly responsible.”

The “catch” portion of the “peculiarly responsible” definition applies to the design of the 2”x 2” heat sink. Under the proposed definition, an item is:

> “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions” if it is used in or for use in the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an item subject to the EAR….

Here, the heat sink is used in a 4A003.b computer, and the design information (i.e., “technology”) for the heat sink is used in the creation (i.e., “development” or “production”) of a 4A003.b computer. Therefore, its design information falls within the scope of the “peculiarly responsible” definition.

However, the “release” portions of the “peculiarly responsible” definition do not apply to the design “technology” of the heat sink for the 4A003.b computer. Under the proposed definition,

“technology” meeting the first part of the definition is controlled under the applicable ECCN (in this example, 4E001) unless:

> (1) The Department of Commerce has determined otherwise in a commodity classification determination;
>
> (2) [Reserved];
>
> (3) It is identical to information used in or with a commodity or software that: (i) Is or was in production (i.e., not in development); and (ii) Is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons;
>
> (4) It was or is being developed with ‘‘knowledge’’ that it would be for use in or with commodities or software: (i) Described in an ECCN; and (ii) Also commodities or software either not enumerated on the CCL or the USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;
>
> (5) It was or is being developed for use in or with general purpose commodities or software, i.e., with no ‘‘knowledge’’ that it would be for use in or with a particular commodity or type of commodity; or
>
> (6) It was or is being developed with ‘‘knowledge’’ that it would be for use in or with commodities or software described: (i) In an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or (ii) Exclusively for use in or with EAR99 commodities or software.

Assume that number (1) does not apply because no commodity classification determination has been sought by Heats Inc. for its 2” x 2” heat sink design “technology.”

Number (3) would not apply to the 2” x 2” heat sink design because its design is not *identical* to the EAR99 design of the 1” x 1” heat sink. The former is an inch greater in length and width. The design information (i.e., “development” or “production” “technology”) for the two types of heat sinks would reflect this difference in physical dimensions even if everything else about them is the same.

Number (4) would not apply to the 2” x 2” heat sink design because the larger heat sink is only being used on 4A003.b computers and was not developed with an intent for or knowledge of use on 4A994 computers.

Numbers (5) and (6) would not apply to the 2” x 2” heat sink design because Heats Inc. created the larger heat sink at HPC’s request, knows that HPC uses them for 4A003.b computers, and has never intended to sell the larger heat sinks on the general computing market.

Therefore, under the proposed definition of “peculiarly responsible,” Heats Inc. would be compelled to classify the design “technology” of its 2” x 2” heat sink under 4E001.a. This bizarre and unexpected result is not reached under the EAR as it exists today.

The design “technology” of the 2” x 2” heat sink would not be controlled under the current definition of the term “required.” 4A003.b applies to computers whose “Adjusted Peak Performance” exceeds 8.0 weighted TeraFLOPS (“WT”), as calculated by a formula provided in Category 4 of the Commerce Control List (CCL). The WT value of a computer is a function of its processors’ architectures (such as 64-bit floating point operations) and speed (i.e., frequency), as well as the aggregation of the computer’s processors as calculated under the WT formula in Category 4 of the CCL. Today, an exporter can satisfactorily resolve the heat sink design technology classification question under the existing definition of “required,” which controls:

> … only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions…. For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are “required” to make the controlled product and are themselves controlled under the General Technology Note.

In the Heats Inc. hypothetical, the heat sink in the 4A003.b computer has no impact on the latter’s WT calculation. Nothing about the heat sink can alter the variables that contribute to a computer’s WT value. The heat sink cannot, for instance, make the computer run another 64-bit floating point operation; it has no bearing on integrated circuit architecture. The heat sink design cannot make the computer’s microprocessors run at a higher frequency than the processor’s silicon will naturally support. The presence of a heat sink in a computer does not result in the aggregation of multiple microprocessors under Category 4’s WT formula. The heat sink thus has no causal relationship whatsoever with the variables that determine computer’s WT value; i.e., the heat sink has no ability to make a computer achieve or exceed its controlled performance level of 8.0 WT. Therefore, the heat sink is not peculiarly responsible for HPC’s computers achieving or exceeding that performance threshold, and the design of the 2” x 2” heat sink would thus not be controlled under 4E001 today. Rather, the heat sink design would be classified as EAR99 “technology,” which is a reasonable, common-sense outcome.

B. Example 2: Motherboard Design “Technology”

Consider another example involving two different motherboard manufacturers, Mobo One and Mobo Two, and two microprocessor manufacturers, CPU-A and CPU-B. Mobo One has

designed a four-socket motherboard for a computer using four microprocessors from CPU-A, and the resulting system falls below 8.0 WT. Assume that Mobo Two has designed a four-socket motherboard for a computer using four microprocessors from from CPU-B, and with CPU-B's superior microprocessors, this system reaches 8.1 WT and is thus classified under 4A003.b.

Here, Mobo Two's motherboard design "technology" is "caught" under the proposed definition of "peculiarly responsible" because the board design "technology" is "used in or for use in" the "development" or "production" of a 4A003.b computer.

It is not difficult to imagine a set of business circumstances that fail all of the "release" provisions in the proposed definition of "peculiarly responsible." Maybe Mobo Two is designing the motherboard only for this specific model of processor from CPU-B such that this board design is not completely identical to a board already in mass production for computers classified under 4A994 (even if those differences are trivial in nature, such as the location of a USB port or placement of a single resistor). Maybe the customer's delivery schedule requirements make it impractical for Mobo Two to obtain a commodity classification determination prior to designing and manufacturing the motherboard that uses CPU-B's processors. In this example, applying the proposed definition of "peculiarly responsible" would produce a "catch" but not a "release," making the board design constitute 4E001 "technology," which is an improper result because the motherboard has no ability to modify the technical parameters that can make a computer fall within the scope of 4A003.b. I.e., motherboard design is orthogonal to the WT value of a computer. For example, a motherboard cannot perform a 64-bit floating point operation. A motherboard cannot enable a microprocessor to run at a higher frequency than the silicon itself will allow. The board design information (i.e., "technology") does not have any unique properties "for achieving or exceeding the controlled performance levels, characteristics or functions" of a 4A003 computer. In this example, it is simply a coincidence that CPU-B's microprocessors drive the system above the 8.0 WT control threshold. The motherboard could theoretically have been tweaked to accommodate another company's lower-performing microprocessors. Business circumstances simply did not lead to that fate. Therefore, there is not a good reason to treat information about Mobo Two's board design as controlled 4E001 "technology."

Many similar examples could be found for a wide variety of technologies.

C. The Proposed Definition Is Inconsistent With The General Technology Note

Exclusion (4) in the proposed definition of "peculiarly responsible" is inconsistent with the text of the General Technology Note. In Supplement No. 2 to Part 744 of the EAR, the General Technology Note states that:

> "Technology" "required" for the "development", "production", or "use" of a controlled product remains controlled **even when applicable to a product controlled at a lower level**. (Emphasis added.)

However, exclusion (4) in the proposed definition of "peculiarly responsible" would not control "technology" if:

> It was or is being developed with ''knowledge'' that it would be for use in or with commodities or software: (i) Described in an ECCN; and (ii) Also commodities or software either not enumerated on the CCL or the USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons….

If BIS adopts its proposed definition of "peculiarly responsible," we encourage BIS to resolve this inconsistency, which would likely be a source of confusion for exporters. However, Google recommends simply not adopting a specific definition for the term "peculiarly responsible" and continuing to use the existing definition of "required," which provides adequate guidance to satisfactorily resolve the vast majority of classification decisions and causes no conflict with the General Technology Note.

D. Recommendations For Alternative Definition

Google's preference is for BIS not to define the term "peculiarly responsible." Any benefits it would provide in terms of clarity are outweighed by detriments it would cause by controlling some technologies unnecessarily. However, if BIS insists on creating a specific definition for the term, then it could improve the definition by the following:

1. Amend the third exclusion to read: "It is identical or substantially similar to information used in or with a commodity or software that is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons." Please note that this recommendation also removes the proposed definition's clause "Is or was in production (*i.e.*, not in development)." If a piece of information is unrelated to the technical reasons for an end-item's control, it should not matter that the information also relates to an item manufactured at a sufficient volume to constitute "production" as opposed to "development." It is unclear how the distinction between "development" and "production" provides a reasonable basis for potentially controlling information that is orthogonal to the reason(s) for an item on the CCL being controlled.
2. Otherwise clarify that information (i.e., "technology") is not "peculiarly responsible" and thus not controlled if it does not have any causal impact on the technical performance levels or characteristics that the CCL uses to capture an end-item.

Definition of “Required”

If BIS establishes a formal definition of the term “peculiarly responsible,” then it should place this term in quotation marks when it appears in the definition of the word “required” so that exporters will know that they should cross-reference the definition of “peculiarly responsible.” Otherwise, readers of “required” will not necessarily be aware that they need to consult both definitions in order to resolve their classification issues.

Additionally, if BIS creates a formal definition of the term “peculiarly responsible” and does not incorporate any of the suggestions that we have recommended above for that term, then it should eliminate from the definition of “required” the illustration regarding technologies “A,” “B,” “C,” “D,” and “E” for a widget operating at or above 400 MHz. This illustration within the definition of “required” does not contain sufficient factual detail to establish clearly that technologies A through C are not “peculiarly responsible” under the “catch and release” analysis proposed for that term, especially the “releases” in numbers (1) through (6) of the proposed “peculiarly responsible” definition. This inconsistency between proposed definition of “peculiarly responsible” and the existing example within the term “required” indicates a deficiency in the former. If the proposed “peculiarly responsible” term is not rejected -- or at least significantly altered, the illustration is incomplete at best, misleading at worst, and should be removed from the definition of “required.”

Definition of “Technology”

Proposed § 772.1 of the EAR includes in its definition of “technology”:

> (a)(5) Information, such as decryption keys, network access codes, or passwords that would allow access to other “technology” in clear text or “software.”

If a decryption key (or other means of accessing materials in clear text) is treated as “technology,” making the key publicly available would remove the key from the scope of the EAR. If the key is no longer subject to the EAR, what is the consequence, if any, to the classification of the material that it decrypts? E.g., would that encrypted material also become publicly available and removed from the scope of the EAR (regardless of whether the clear text of the encrypted material has directly been made publicly available)?

Definition of "Export"

A. BIS should delete the term "or permit" from proposed § 734.13(a)(6).

Proposed § 734.13(a)(6) defines as an export:

> Releasing or transferring decryption keys, network access codes, passwords, software, or other data with “knowledge” that such provision will cause **or permit** the transfer of other technology or software in clear text to a foreign national.” (Emphasis added.)

Now consider the following key or password:

> E2ArxmM6kKxPzSADzcQK

It is a logical truth -- and, therefore, we have knowledge -- that this string of numbers and letters permits any person, including foreign nationals, to access in clear text any technology or software that has been protected by the code “E2ArxmM6kKxPzSADzcQK.” However, we have no idea whether any technology or software in the world actually exists that is protected by this random string of numbers and letters. Furthermore, we have no idea what ECCNs may apply to such technology or software. By their very nature, decryption keys, network access codes, passwords, and the like permit access to their associated protected material. Any transfer of decryption keys, network access codes, passwords, etc. would necessarily result in knowing that access to the protected materials has been permitted (i.e., theoretically allowed).

We are also concerned about the fundamental fairness of BIS creating liability for merely permitting a technology or software transfer if no actual (or high probability of an actual) violation occurs. For instance, consider a situation where a simple administrative error takes place and a foreign person is temporarily given access to a system that would theoretically permit this person to access controlled technology or software. As a matter of fairness and as a measure of actual harm, it is materially different comparing a situation where this foreign person were actually to view or download controlled technology or software before the administrative error was detected with another situation where the foreign person merely had access for a period of time but never actually viewed or downloaded controlled material. If no transfer of technology or software takes place, an “export” should not be established under the EAR.

Accordingly, BIS should delete the term "or permit" from proposed § 734.13(a)(6).

B. BIS should add the modified "knowledge" provisions of proposed § 734.13(a)(6) to the deemed export rule in proposed § 734.13(a)(2).

Proposed § 734.13.(a)(6) defines as an export:

> Releasing or transferring decryption keys, network access codes, passwords, software, or other data with “knowledge” that such provision will cause or permit the transfer of other technology or software in clear text to a foreign national.

Proposed § 734.13.(a)(2) defines as a deemed export:

> Releasing or otherwise transferring “technology” or “source code” (but not “object code”) to a foreign national in the United States (a “deemed export”).

The definition of "technology" in proposed § 772.1(a)(5) includes "[i]nformation, such as decryption keys, network access codes, or passwords that would allow access to other ‘technology’ in clear text or ‘software.’" Therefore, any transfer of a decryption key, etc. to a foreign national in the United States would be treated as a deemed export.

We request that BIS make § 734.13(a)(2) consistent with (a)(6) and include an equivalent "knowledge" requirement. The rationale for including a "knowledge" requirement in (a)(6) -- and limiting it to "knowledge" of actual, not theoretical, access to controlled materials -- is identical to requiring "knowledge" of actual, not theoretical, access to controlled "technology" or "source code" for purposes of a deemed export.

Accordingly, § 734.13(a)(2) should be changed to read:

> Releasing or otherwise transferring “technology” or “source code” (but not “object code”) to a foreign national in the United States (a “deemed export”). Releasing or transferring decryption keys, network access codes, passwords, software, or other data is a deemed export when made with “knowledge” that such provision will cause the transfer of other technology or source code in clear text to a foreign national.

Definition of Reexport & Deemed Reexport

The comments and recommendations above regarding "export" and "deemed export” also apply to the proposed definitions of "reexport" and "deemed reexport."

Activities That Are Not Exports, Reexports, Releases, Retransfers, or Transfers

Proposed § 734.18(a) lists a number of activities that are not treated as exports, reexports, or transfers for purposes of the EAR. Proposed § 734.18(a)(4) includes sending, taking, or storing “technology” or “software” that is, among other things, secured using 'end-to-end encryption.' Proposed § 734.18(b) states that "‘end-to-end encryption’ means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where 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."

Although the creation of this exclusion from the scope of the EAR is useful, it is unlikely to be used widely. End-to-end encryption as described by the proposed regulation is relatively uncommon in cloud computing environments. Where it exists, it is used most frequently in cloud

storage services. However, it does not even represent the majority of usage in cloud storage environments. Outside of cloud storage, end-to-end encryption is found even less frequently in the provision of cloud-based services. Introducing end-to-end encryption to cloud services often results in the loss of too many useful features desired by cloud computing customers. For instance, in cloud-based email systems, it would result in the loss of features like search, spell check, and spam detection. Accordingly, the overwhelming majority of cloud computing providers, users, and uses will fall outside the scope of proposed § 734.18. The proposed regulation does not make clear how it intends to treat cloud transactions in environments that do not use end-to-end encryption. Based on conversations with BIS, however, our understanding is that those transactions would be governed by the existing advisory opinions that BIS has issued on cloud computing, which industry has relied upon for the last several years.

Thank you for your consideration. Please do not hesitate to contact us via email (neilmartin@google.com) or phone (650-253-1816) with any questions or comments regarding this submission.

Respectfully,

Neil Martin

Export Compliance Counsel
Google Inc.