Office of Chief Counsel
Internal Revenue Service
Memorandum

Number: **AM2016-004**
Release Date: 10/14/2016

CC:INTL:MARollinson
POSTU-103801-16

UILC: 6103.11-00, 6105.00-00

date: June 17, 2016

to: John M. Dalrymple
Deputy Commissioner for Services and Enforcement

from: Marjorie A. Rollinson
Associate Chief Counsel
(International)

---

subject: **OECD COMMON TRANSMISSION SYSTEM (CTS) -- RESPONSIBILTY FOR DATA TRANSMITTED UNDER SECTION 6103 AND 6105, AND TAX TREATIES**

The Commissioner requested written advice regarding the issue of when legal responsibilities to protect tax return information arise in the context of electronic data transmission through the Common Transmission System (CTS). The CTS is a "global" transmission system being developed under the Organization for Economic Cooperation and Development (OECD) Forum on Tax Administration (FTA).[1] The purpose of the CTS will be to facilitate the automatic exchange of financial account information, "country-by-country" reporting,[2] and other exchanges of information between tax administrations. This advice addresses data transmitted via the CTS to the IRS from

---

[1] The FTA is a forum on tax administration for Commissioners from 46 OECD and non-OECD countries, including every member of the G20. Some of the primary purposes of the FTA are to create a forum through which Commissioners can identify, discuss and influence relevant global trends and develop new ideas to enhance tax administration around the world.

[2] The OECD's Base Erosion and Profit Shifting (BEPS) Project, Action Plan 13, includes a requirement that multinational enterprises (MNEs) report to their tax administration their business activities using an agreed-upon template on a country-by-country basis. The country-by-country report will contain certain information relating to the global allocation of the MNE group's income and taxes paid, together with certain indicators of the location of economic activity within the MNE group. It is anticipated that tax administrations will then exchange this information with each other as appropriate.

foreign tax administrations (inbound transmissions) and data sent by the IRS to foreign tax administrations (outbound transmissions).[3]

As a preliminary matter, it is noted that the factual description of the CTS contained in this advice, including with regard to the scope, legal framework, and key technical features of the CTS, [redacted] are based on information and representations provided by the OECD. Since the CTS project is still ongoing, Counsel is not able to confirm that the transmission system will, in fact, be constructed as described by the OECD, although all indications currently are that it will be. Further, this advice does not purport to make any legal conclusions on the adequacy for, or satisfaction of, any other pertinent requirements or rules such as, but not limited to, requirements similar to those under FISMA or NIST, or other requirements determined to be necessary in order for the IRS to use the CTS.

This written advice was prepared in conjunction with the Office of Associate Chief Counsel (Procedure and Administration), and coordinated with the Office of the Associate Chief Counsel (General Legal Services) and key stakeholders in Large Business and International (LB&I).

I. EXECUTIVE SUMMARY

In light of recent global developments in the areas of transparency and exchange of information, and recognizing that automatic exchanges of information between tax administrations will likely increase over the coming years, the OECD is developing a common system for transmissions of data between governments. The projected increase in the number of automatic exchanges of information is due, in large part, to the OECD's "Standard for Automatic Exchange of Financial Account Information in Tax Matters" (a/k/a, "Common Reporting Standard" or "CRS"), which provides for automatic exchanges of financial account information, and the output of Action Plan 13 of the OECD's Base Erosion and Profit Shifting (BEPS) Project, which calls for automatic exchanges of "country-by-country" reports. The development of a common solution for the transmission of data in the form of the CTS was viewed by the OECD as well as member jurisdictions of the FTA as an efficient and economically beneficial way to accommodate the global needs in the area of automatic exchange of information.

We have been asked to opine on the moment during the exchange of information via the CTS when information becomes protected under the various sources of statutory and tax convention protection from disclosure.

Returns, return information, and tax convention information are categories of information related to taxes that are generally protected from disclosure under Internal

[3] It is our understanding that if the IRS adopts the CTS, IDES may continue to be used for exchange of information with third parties; for example, to permit direct reporting non-financial foreign entities to provide financial account information directly to the IRS.

Revenue Code sections 6103 and 6105. Data transmitted via the CTS will fall within one or more of these categories. In addition, the language of the United States' bilateral and multilateral tax conventions, tax information exchange agreements, as well as intergovernmental agreements concerning the implementation of FATCA all contain provisions concerning the obligation to protect covered information from disclosure.

Briefly, information that will be transmitted by the IRS to foreign tax administrations (outbound transmissions) through the CTS is return information under section 6103 in the hands of the IRS, so throughout the exchange process should be protected as required by section 6103. Furthermore, that information becomes treaty-protected information in the hands of the foreign country when the information is exchanged pursuant to a tax convention or other international agreement on taxes.

In the case of information provided to the IRS by foreign tax administrations (inbound transmissions) through the CTS, the moment when legal protection arises is less certain. While there are two moments when legal protection could arise in an inbound transmission (i.e., the moment information is uploaded to the CTS by the foreign tax authority, and the moment when the United States downloads the information from the CTS), we believe the most likely moment is when the United States downloads the information from CTS.

There is no direct authority regarding the precise moment legal protection arises. However, close reading of the various statutory and tax convention language, as well as related court decisions seem to indicate that protection will not arise until the information is actually held by the IRS.

As discussed in this advice, the CTS is different from the International Data Exchange Service (IDES), which is a system funded, designed, and managed by the IRS. In a prior memorandum, we concluded that information transmitted via IDES by a foreign jurisdiction to the United States would most likely be treated as gaining section 6103 protection upon upload to IDES. The CTS is not a U.S.-designed system. The OECD, and not the IRS, will negotiate the agreement with the CTS vendor; and the costs associated with the development and operation of the CTS will be borne by all users globally and not just by the IRS. Therefore, our view is that with regard to information transmitted to the IRS through the CTS, section 6103 protection arises when the information is downloaded by the IRS. It is our understanding that if the IRS adopts the CTS, as a matter of convenience to the IRS, the IRS will continue to use IDES as a regional router in order to facilitate exchanges of information via the CTS. Therefore, with regard to inbound transmissions to the IRS, section 6103 protection arises when the information is uploaded from the CTS to IDES.

Furthermore, we believe section 6105 and treaty protections are likely to follow the conclusion under section 6103. In other words, with regard to inbound transmissions to the IRS, the protection under section 6105 and tax conventions arise, not when the data

is uploaded to the CTS by the foreign tax administration, but only when the data is uploaded to IDES from the CTS.

II. COMMON TRANSMISSION SYSTEM (CTS)

The discussion in this memorandum of the proposed model for the CTS is based [redacted] on information contained in [redacted] the "Call for Tenders", particularly the section on functional and service requirements of the CTS.

A. Scope of the CTS

Currently, the scope of the CTS is the actual transmission of data between tax administrations. It can be viewed as the "pathway" to facilitate government-to-government exchanges of information. Therefore, the scope of the CTS does not include data storage or file preparation prior to the sending of the information or any processes following the receipt of the data (e.g., relating to encryption/decryption, compression, storage, etc.).

B. Vendor Agreement and User Agreements

The proposal is that the OECD will negotiate and conclude an agreement with the selected vendor[4] to develop, maintain, and provide ongoing support for the CTS (Vendor Agreement). The OECD will also conclude agreements with each of the jurisdictions that will use the CTS (User Agreement). The negotiation process for the Vendor Agreement and the User Agreements has begun. It is anticipated the Vendor and User Agreements will be concluded by mid-2016. The OECD advised that there will be some opportunity for jurisdictions to provide input during the negotiation process. [redacted]

C. Key Technical Features

The [redacted] CTS will be built to ensure the security and safeguarding of the data at all times. All data transmitted must be properly encrypted

[4] For purposes of this memorandum, the term "vendor" includes the contactor, subcontractor(s), and any CTS development partner(s) as described in the vendor proposal.

prior to transmission.[5] Only data that has been properly encrypted will be accepted by the CTS, since the CTS will be built to immediately delete or reject any unencrypted file that is uploaded. With the exception of the "metadata" (e.g., the IP address where the information is to be delivered), the CTS itself will not be able to read the data being transmitted, nor will the vendor have any access to the data. Further, the transmission pathway will also be encrypted, which would include encrypting the metadata. Since the data package being transmitted will be fully encrypted, only the sending and receiving jurisdictions will have the ability to access and encrypt/decrypt the information contained in the data package. It is envisioned that the jurisdictions involved in the exchange of information will provide each other with their respective unique digital certificates ("keys") necessary to encrypt/decrypt the information being exchanged.[6]

The CTS is envisioned to allow a recipient jurisdiction to choose whether the information is to be sent directly from the CTS platform to its system as soon as the data is uploaded by the sender (the "push model"), or whether the information would be temporarily held in the CTS for the recipient jurisdiction to retrieve at a time of its choosing (the "pull model"). The stated reason for this flexibility was to accommodate jurisdictions with less capacity to be able to exercise control over when their server space would be required to receive the information. [redacted]

The [redacted] CTS will have the ability to verify the identity of users and to ensure that access is limited to authorized users (i.e., "identity and access management"). Further, a jurisdiction using the system will have the ability to define specific recipients within its tax administration (e.g., certain roles and areas of responsibility) to receive particular transmissions depending on the type of information being exchanged, including any responses or other notifications being sent to the specified user.

Regarding the supervision and reporting features of the CTS [redacted], some of the features that relate to data security are as follows:

- There will be an ongoing diagnosis and resolution of connectivity and transmission issues, including issues in relation to data security;

[5] [redacted]

[6] [redacted]

- The system will monitor access through audit logging and such logs will be available to users;
- The system will maintain information on the identification of users, and the time, date, and activity of users; and
- The system will automatically notify users of any successful, unsuccessful, and retry transmissions and can provide users with information about the number and size of files sent, the transmission time, and the result of the transmission.

[redacted]

[redacted][7]

[redacted][8]

[redacted]

[redacted]

[7] The FTA Informal Transmission Group is a group of representative jurisdictions (including the United States), large and small, developed and less-developed, OECD and non-OECD, set up by the FTA specifically to explore development of the CTS.

[8] The Global Forum has been the multilateral framework within which work in the area of transparency and exchange of information has been carried out by both OECD and non-OECD economies since 2000. The Global Forum currently includes 126 member jurisdictions and the European Union, together with 15 observers.

[redacted]

III. LEGAL FRAMEWORK - SECTIONS 6103 AND 6105, AND TAX TREATY CONFIDENTIALITY

A. Section 6103

Section 6103(a) of the Internal Revenue Code (Code) provides the general rule that returns and return information must be kept confidential and can only be disclosed as authorized under the Code. The term "return" means any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the Code which is filed with the IRS by, or on behalf of, any person. I.R.C. §6103(b)(1). Section 6103(b)(2) defines return information broadly to include the taxpayer's identity and any taxpayer-related information that is "received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of" tax liability. Return information does not include data in a form that cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. I.R.C. § 6103(b)(2). Under section 6103(b)(8), the term "disclosure" means the making known to any person in any manner a return or return information.

One exception to the general confidentiality rule of section 6103(a) is found in section 6103(k)(4), which provides that "return or return information may be disclosed to a competent authority of a foreign government which has an income tax or gift and estate tax convention or other convention or bilateral agreement relating to the exchange of tax information with the United States but only to the extent provided in, and subject to the terms and conditions of, such convention or bilateral agreement."

Section 6103(p)(4) sets forth technical, administrative, and physical safeguard provisions that prohibit certain statutorily-described recipients of returns and return information from using or disclosing such information in an unauthorized manner and requires recipients to store returns and return information in a secure area or place. The section 6103(p)(4) safeguard provisions do not apply, however, with respect to section 6103(k)(4) disclosures. Regarding section 6103(k)(4) disclosures, the exchange of information agreements themselves contain strict confidentiality rules that limit disclosure and use of the information exchanged.[9] Further, section 6105 provides for confidentiality of tax convention information as discussed later in this memorandum.

[9] The *U.S. Model Income Tax Convention* (U.S. Model) provides, in Article 26, that information received by a Contracting State "shall be treated as secret … and shall be disclosed only to persons or authorities (including courts and administrative bodies) involved in the assessment, collection, or administration of, the enforcement or prosecution in respect of, or the determination of appeals in relation to [covered taxes] …. Such persons or authorities shall use the information only for such purposes." The tax treaties and tax information exchange

i. Case Law Interpreting Section 6103

Case law has addressed *what* information is protected by section 6103, but does not directly address *when* information begins to be protected by section 6103. For instance, in *Landmark Legal Foundation v. IRS*, 267 F.3d 1132 (11th Cir. 1996), the Eleventh Circuit addressed the appropriate scope of an IRS claim that information constituted "return information." In that case, the appellant sought to overturn the district court's holding that identities of third parties who requested audits or investigations of certain tax-exempt entities and the content of those requests constituted return information under section 6103(b)(2)(A). The Eleventh Circuit rejected the appellant's argument that the identities and requests were not "data" or "received by . . . [the IRS] with respect to a return or with respect to" any issue. *Id.* at 1136. The Eleventh Circuit concluded that the "deliberately sweeping" language of section 6103 reached any data "received by, recorded by, prepared by, furnished to, or collected by" the IRS and whether or how the IRS used that data once it arrived was irrelevant to its status as return information. *Id.* Similarly, in *Hull v. IRS*, 656 F.3d 1174, 1187 (10th Cir. 2011), citing *Landmark Legal Foundation*, the Tenth Circuit found that whether the IRS actually "used" the information at issue was immaterial; what mattered was that the information was received by the IRS with regard to the possible existence of a tax liability. However, neither opinion addresses exactly when the data became "return information."

There is broad consensus that to be protected by section 6103, information must be possessed in some manner by the IRS. For instance, the Eleventh Circuit has clarified that "the statutory definition of 'return information' confines it to information that has passed through the IRS." *Ryan v. U.S.*, 74 F.3d. 1161, 1163 (11th Cir. 1996). In that case, an IRS special agent assisted the U.S. Attorney's Office in collecting certain information related to a criminal investigation. Because the U.S. Attorney's office itself had sought and received that information, not the IRS, the information did not belong to the IRS and therefore was not return information protected by section 6103. *See also Stokwitz v. U.S.*, 831 F.2d 893 (9th Cir. 1987), *cert. denied*, 485 U.S. 1033 (1988). In *Stokwitz*, a case cited approvingly by *Ryan*, Naval investigators searched a personal office, discovered personal copies of income tax returns filed with the IRS, and subsequently disclosed information from those returns. The Ninth Circuit held that because the copies of the income tax returns were not obtained as a result of those materials being filed with the IRS, they were not protected by section 6103. Section 6103 "is concerned solely with the flow of tax data to, from, or through the IRS." *Id.* at 896. Similar distinctions are also followed by the Fifth Circuit. *See Baskin v. U.S.*, 135 F.3d 338, 342 (5th Cir. 1998) ("[T]o be 'return information' any information must first be 'received by, recorded by, prepared by, furnished to, or collected by' the IRS. The plain

---

agreements (TIEAs), as well as the IGAs, to which the United States is a party contain similar language with regard to confidentiality of the information exchanged.

language of the statute reveals that 'return information' must be information which has somehow passed through, is directly from, or generated by the IRS.").

ii. Unlawful Disclosures of Section 6103 Data

Section 7431(a)(1) provides for civil damages due to willful or negligent inspections or disclosures by U.S. government employees of any return or return information in violation of section 6103. Section 7431(a)(2) provides similar sanctions for willful or negligent inspections of return information by non-government persons. Section 7431(b)(1) provides an exception for inspections or disclosures that result from a good faith, but erroneous interpretation of section 6103. Section 7431 has a criminal counterpart in section 7213, which provides for criminal sanctions based on the willful inspection or disclosure by U.S. government and non-government persons of any return or return information in violation of section 6103.

B. Section 6105 and Tax Treaty Confidentiality

In addition to the protections under section 6103, information received from a foreign government pursuant to a tax convention is also subject to the confidentiality rules of section 6105. Section 6105(a) contains the general rule that tax convention information must not be disclosed unless it falls under one of the exceptions listed in section 6105(b). The terms "tax convention information" and "tax convention" are defined in sections 6105(c)(1) and (c)(2), respectively. In general, tax convention information subject to the protection of section 6105(a), includes information exchanged pursuant to a tax treaty or other bilateral agreement (including multilateral conventions) providing for the exchange of information which is treated as confidential or secret under the relevant convention or agreement. Therefore, information that is exchanged (transmitted through CTS) with a foreign tax administration under a tax treaty, TIEA, or an IGA will be subject to the protections of section 6105.

The legislative history under section 6105 does not describe when information becomes tax convention information. There is very sparse case law under section 6105 and the treaties, and it does not address the timing of when protection arises.

As previously discussed, each of the tax treaties, TIEAs, as well as the IGAs to which the United States is a party, include confidentiality provisions that require all information exchanged to be kept confidential in accordance with the provisions of such treaty, TIEA, or agreement, as well as provisions generally limiting the use of the information only for purposes of tax administration. The explanation of Article 26 (addressing exchange of tax information between countries) of the U.S. Model (and corresponding model under the OECD) does not shed light on the exact moment when the duty to protect treaty exchanged information arises. Where terms are otherwise undefined under a treaty, or by mutual agreement by the competent authorities pursuant to a

treaty, they have the meaning that is assigned to that term under the law of the country for the purposes of the taxes to which the treaty applies.[10]

[redacted][11] Unlike IDES, however, the CTS is not a U.S.- designed system; and as discussed above, the OECD, and not the IRS, will negotiate the agreement with the vendor. Further, the costs associated with the development and operation of the CTS will be borne by all users globally and not just by the IRS. [redacted]

IV. APPLICATION OF LEGAL PRINCIPLES TO CURRENT FACTS

To analyze when section 6103, section 6105, and treaty, TIEA, or IGA protection applies, it is helpful to separately consider the outbound and inbound transmission of data. Outbound transmission is the transmission of data held by the IRS through the transmission system to a foreign tax administration. Inbound transmission is the submission of data to the IRS by a foreign tax administration.

A. Application of Section 6103 to Outbound Transmissions

In the case of outbound transmissions, the IRS already possesses the data to be transmitted; therefore, that data already constitutes return or return information within the meaning of sections 6103(b)(1) and (b)(2). Consequently, the IRS is responsible for taking appropriate steps to protect the data when it is uploaded for transmission to the CTS. The IRS must also have statutory authority under section 6103 in order to transmit the data to its ultimate recipient.

i. Uploading Section 6103 Data to the CTS

[10] See, for example, Article 3 section 2 of the U.S. Model.

[11] The "IDES memo," dated June 9, 2015, was prepared by Counsel in response to the Commissioner's request for written advice regarding when the legal responsibilities to protect tax return information arise in the context of transmission of data through IDES. (GLAM (AM2015-005 Release Date 7.17.15)).

At the outset, we must determine whether the IRS is authorized to disclose section 6103 data to the CTS itself. Because we conclude that the transmission of the data to the CTS is not itself a "disclosure" for purposes of section 6103, as explained below, the upload of data, even though protected by section 6103, does not need the normal permission under a specific exception under section 6103. Our conclusion rests on the presumption and understanding that the CTS will operate with the requirement that all information transmitted must be encrypted using agreed upon state-of-the art encryption methods, and that the IRS will ensure that such encryption methods are in place and required of all users prior to uploading any data to the CTS.

As stated above, [redacted]all data transmitted through the CTS must be properly encrypted prior to transmission, and only data that has been properly encrypted may be transmitted. With the exception of "metadata," the CTS itself will not be able to read the data being transmitted, nor will the vendor have any access to the data. Further, it is anticipated that the transmission pathway would also be encrypted, which would include encrypting the metadata. Based on the information provided by the OECD regarding how the data, metadata, and the transmission pathway will be encrypted, and the limitations on the vendor's access to the data, we conclude that an upload of encrypted data to the CTS by the IRS in an outbound transmission will not be considered a disclosure for section 6103 purposes to the CTS itself or to the vendor.

Under section 6103(b)(8), the term "disclosure" means the making known to any person in any manner a return or return information. Because of the encryption methods employed by the CTS, and the firm restrictions on the vendor's access to the data flowing through the system, we conclude there would be no "making known" of the uploaded data to the CTS or the vendor. Rather, the CTS may be viewed as a mere conduit for the transmission of the section 6103 data to the recipient foreign tax administration. Consequently, the upload of encrypted data by the IRS to the CTS is not a disclosure to the CTS or the vendor for purposes of section 6103.

ii. Disclosure to Foreign Tax Authority

Even though there is no disclosure for purposes of section 6103 to the CTS or the vendor, the IRS is still making a disclosure of the data to its ultimate recipient and therefore must have the requisite statutory authority to do so. We conclude that under section 6103(k)(4), the IRS may disclose section 6103 data in an outbound transmission to a foreign tax administration, provided the disclosure complies with the requirements of that section. Section 6103(k)(4) allows disclosures of return information to a competent authority of a foreign government which has an income tax or gift and estate tax convention, or other convention or bilateral agreement relating to the exchange of tax information, with the United States, but only to the extent provided in, and subject to the terms and conditions of, such convention or bilateral agreement. Provided the IRS

only transmits information to tax convention, TIEA, or IGA partners and the outbound transmission of section 6103 data is in accordance with the terms and conditions of the applicable convention, TIEA, or IGA, the disclosure of return information via an outbound transmission is permissible under section 6103.

We also note that under the terms of the applicable treaty, TIEA, or IGA governing the exchange of information, the foreign tax administration is, or will be, obligated to protect the data once it has possession of it. Although not mandated by section 6103,[12] the exchange of information agreements themselves contain strict confidentiality rules that limit disclosure and use of the information exchanged (see footnote 9).

In summary, as discussed above, based on the requirement that the data, metadata, and the transmission pathway itself be encrypted, and the restrictions on access to the data as it flows through the CTS, we conclude that the uploading of the encrypted data to the CTS for an outbound transmission by the IRS is not a making known of section 6103 data, and therefore is not a disclosure of return information for section 6103 purposes with respect to the CTS or to the vendor. Rather, the CTS should be viewed as a mere conduit for the outbound transmission of that information. Section 6103(k)(4) permits the IRS to disclose the section 6103 data in an outbound transmission through the CTS to the recipient foreign tax administration, provided such disclosure is in accordance with the applicable agreement governing the exchange of information.

B. Application of Section 6103 to Inbound Transmissions

Unlike outbound transmissions through CTS, in which the data is protected by section 6103 from the outset, in an inbound transmission the precise moment when section 6103 applies is less clear. However, consistent with the discussion above that returns or return information are not protected under section 6103 until such returns or return information have been possessed in some manner by the IRS, and for the reasons described below, we conclude that section 6103 applies in an inbound transmission to the IRS upon upload of the data from CTS to IDES.

It is our understanding that if the IRS adopts the CTS, IDES may continue to be maintained to allow for exchange of information with third parties; and further, as a matter of convenience, the IRS may continue to use IDES as a regional router[13] in order to facilitate exchanges of information with foreign tax administrations via the CTS. In an outbound transmission, the IRS will first upload data onto IDES where it is then uploaded onto CTS from IDES, and ultimately transmitted to the recipient foreign tax administration. In an inbound transmission, the foreign tax administration will first

[12] The section 6103(p)(4) safeguard provisions do not apply with respect to section 6103(k)(4) disclosures.

[13] A "regional router" is a managed file transfer system that serves as an intermediary between the sending and receiving jurisdictions. For example, if a regional router is used by Country A in connection with the CTS, the data file being transmitted by Country A will pass to the regional router before it is uploaded to the CTS; and likewise, information being transmitted to Country A will be uploaded by the CTS to the regional router.

upload its data onto CTS, where it is then uploaded onto IDES from the CTS, before being downloaded onto the IRS's internal computers. To facilitate these exchanges, the IRS plans to use a computer-to-computer[14] model, similarly to how it operates IDES, whereby the IRS's internal computers communicate directly with the IDES system, and any data that is uploaded onto IDES (via the CTS) by a foreign sender will be instantaneously downloaded onto the IRS' internal computers.[15]

In the IDES memo, we concluded that section 6103 applies once data is uploaded onto IDES during an inbound transmission to the IRS. In the IDES memo, it was decided that section 6103 protection, with respect to inbound transmissions, arises when the data is uploaded onto IDES by a foreign tax administration. [redacted]

We reach a similar conclusion here. When the data is uploaded onto IDES from the CTS during an inbound transmission to the IRS, it becomes protected by section 6103.[16] Unlike IDES, CTS will not be designed, solely funded, and controlled by the IRS. CTS will act as a mere transmission pathway for exchanges of information between the foreign tax administration and the IRS. The agreement or contract to operate the CTS will be between the OECD and the vendor; in turn, the OECD will conclude agreements with each tax authority that plans to send or receive data through the CTS. The OECD will charge and collect fees from each tax authority based on usage of the CTS. [redacted][17]

[14] A "computer-to-computer" transmission is one that is entirely automated. The data is sent by an application through the Secure File Transfer Protocol ("SFTP") communication channel and received and downloaded by the recipient in the same fashion. In other words, there is no human involvement at any step of the process.

[15] [redacted]

[16] Even though we conclude that section 6103 protection does not apply to data in an inbound transmission until the data is uploaded to IDES from the CTS, it is presumed that the sending country in an inbound transmission will take the appropriate steps to ensure that the data being uploaded to CTS adheres to the requisite encryption methodologies. Note that a key technical feature of CTS is that it will immediately delete or reject any unencrypted file that a user attempts to upload. Therefore, if a sending country attempts to send data to the IRS that is not properly encrypted, it will not be able to so. Furthermore, the IRS has an interest in ensuring that the CTS meets the requisite encryption methodologies in order for the IRS to be able to send 6103 data in an outbound transmission. In this way, the IRS also ensures that inbound transmissions are likewise secured.

[17] [redacted]

C. Section 6105 and Tax Convention Considerations

Information exchanged between governments using the CTS would be covered by confidentiality protections contained in the exchange of information articles of the applicable tax convention, TIEA, or IGA,[18] and by consequence, under section 6105. Under the statutory language of section 6105(c)(1)(E), information becomes tax convention information when it is "exchanged pursuant to a tax convention which is treated as confidential or secret under the tax convention," and arguably, the use of the past tense "exchanged" suggests that section 6105 protection will not arise for this class of tax convention information until the exchange is completed. Therefore, it is also arguable that information uploaded by the foreign tax administration to the CTS is not fully exchanged until it is actually uploaded to IDES from the CTS (or, if the IDES is not used as a regional router, when the information is downloaded by the IRS directly from the CTS). Article 26, section 2, of the U.S. Model contains a similar past tense usage: "Any information received under this Article … " (emphasis added). Consequently, similar inferences might be drawn from the language of the U.S. Model.

As discussed in the IDES memo, the current terms of the CAA allocate to the United States the risk and obligation to protect information once it is successfully uploaded to IDES by the IGA partner tax administration. Unlike IDES, however, the CTS is not a U.S.-designed system; as discussed above, the OECD, and not the IRS, will negotiate the agreement with the vendor; and the costs associated with the development and operation of the CTS will be borne by all users globally and not just by the IRS. Consistent with the analysis that section 6103 protection arises in an inbound transmission when the data is uploaded to IDES from the CTS (or, if IDES is not used as a regional router, when the IRS downloads the data directly from the CTS), it is our view that section 6105 and confidentiality provisions in our tax information exchange agreements can be interpreted to apply at the same time that section 6103 protections arise. In other words, the protection under section 6105 and tax conventions arise in an inbound transmission, not when the data is uploaded to the CTS by the foreign tax administration, but when the data is uploaded to IDES from the CTS (or, if IDES is not used as a regional router, when the IRS downloads the data directly from the CTS).

[redacted]

[redacted]

[18] See, for example, Article 3 par. 7 of the November 30, 2014 Model 1A IGA for countries with a preexisting double tax convention or tax information exchange agreement. Where the only tax agreement between the countries is the IGA itself, similar provision is made. See Article 3, par. 7 of the November 30, 2014 Model 1B IGA for countries without a preexisting double tax convention or tax information exchange agreement.

[redacted]

[redacted] [19]

[redacted]

[redacted] [20]

---

[19] [redacted]

[20] [redacted]

cc: Drita Tonuzi
Associate Chief Counsel
(Procedure and Administration)

Richard L. Hatfield
Attorney
Office of Associate Chief Counsel
(General Legal Services)

[redacted]