International Data Safeguards & Infrastructure Workbook

United States Internal Revenue Service

March 20, 2014

FOR FATCA IMPLEMENTATION

Table of Contents

1. INTRODUCTION

1.1 Purpose of Document

In light of recent global efforts to combat tax evasion and the development of the intergovernmental approach to implement the Foreign Account Tax Compliance Act (FATCA), there is a greater focus on transparency and the automatic exchange of information. Automatic, or bulk, exchange of tax data differs from exchange based on specific requests. Automatic exchange is performed routinely, and the types of information and timing are agreed to in advance by the parties participating in the exchange of information. Further, information may not necessarily be related to an ongoing investigation or proceeding at the time of the exchange. As a result, it is critical that the source jurisdiction, which is transmitting the information, receives assurance from the receiving jurisdiction that confidentiality of the exchanged information will be upheld, and that the information will be used solely for the purpose for which it is intended.

The United States Department of Treasury has provided five (5) model Intergovernmental Agreements (IGAs) that may be used to implement FATCA depending on the partner jurisdiction's policy and legal environment. In a Model 1A (Reciprocal) Agreement, both the United States and the FATCA Partner agree to exchange information with respect to the residence country's taxpayers' reportable accounts in the source country's reporting Financial Institutions. Before engaging in information exchange with a partner under a Model 1A Agreement, each country will evaluate the other country's exchange of information safeguards as well as the country's infrastructure for an effective exchange relationship.[1]

This International Data Safeguards & Infrastructure Workbook describes the procedures to evaluate a FATCA partner's ability to engage in an effective exchange relationship and adequately safeguard the information exchanged. The guidelines herein can be applicable with regard to exchanges of information under any of the Model IGAs, but they will have particular relevance for jurisdictions signing a Model 1A Agreement with the United States. With regard to a Model 1A Agreement, this Workbook should be applied bilaterally in the evaluation process and produce a single document representing this joint endeavor. Four strategic focus areas will be evaluated as highlighted in Figure 1 (Safeguard Workbook Overview Structure and Guidelines) on the following page: Legal Framework, Information Security Management, Monitoring & Enforcement, and Infrastructure.

[1] The Reciprocal Model 1A Agreement is one of the model intergovernmental agreements published by the Department of the Treasury following the enactment of FATCA. The model agreements were developed to facilitate implementation of FATCA. Further information regarding the model intergovernmental agreements can be found via this hyperlink: U.S. Treasury Resource Center

Figure 1 – Safeguards and Infrastructure Strategic Focus Areas

Data Safeguard Review Phase	Definition	Focus	Examples
1. Legal Framework	▪ Determination of whether the legal framework ensures the confidentiality of exchanged tax information and limits its use to appropriate purposes. The two basic components of such a framework are a country's domestic legislation and the applicable treaty, TIEA, or other bilateral agreement for the exchange of information	▪ Domestic/International provisions requiring the confidentiality of exchanged information to be maintained and used for specified, limited purposes	▪ References to domestic legislation ▪ Terms of applicable treaty, TIEA, or other bilateral agreement for the exchange of information
2. Information Security Management	▪ Comprehensive analysis of a FATCA partner's information security management to determine whether data protection systems for managing EOI, including automatic EOI, are in place	▪ Information security among employees and consultants ▪ Physical security ▪ Information systems security/oversight ▪ Data encryption	▪ Background checks, training, Non-Disclosure Agreements, departure policies ▪ Infrastructure policies ▪ ISO/IEC 27000-series compliance
3. Monitoring & Enforcement	▪ Understanding of process in place to ensure adherence to safeguarding policies and procedures	▪ Mechanisms in place to monitor accesses ▪ Policing of unauthorized disclosures ▪ Penalties and sanctions for improper disclosure or use of taxpayer information	▪ Systems to monitor access ▪ Investigation procedures ▪ Enforcement procedures ▪ Processes for review and approval of recommendations for sanctions / procedural changes
4. Infrastructure	▪ Confirmation that a FATCA partner's infrastructure is in place for an effective exchange relationship	▪ Established processes for ensuring timely, accurate, and confidential information exchanges ▪ Reliable communications approaches ▪ Capabilities to promptly resolve questions/concerns about exchanges ▪ Ability to administer the provisions of the relevant IGA	▪ Collection and transmission of information from Financial Institutions ▪ Prior experience with bulk exchanges ▪ Data validation procedures/ policies for interacting with taxpayers and institutions ▪ Audit policies and procedures

The remaining portion of this introduction discusses the current state of automatic exchange of information, including guidelines provided by the Organization for Economic Cooperation and Development (OECD) on safeguarding data; and the requirements under a Model 1A Agreement for appropriate safeguards and infrastructure to maintain confidentiality of exchanged information. Section 2 of this Workbook discusses the process that an "Evaluating Jurisdiction" will use to review safeguarding procedures, particularly as they relate to automatic exchange; and summarizes elements within the four strategic focus areas to provide clarity for the evaluation questions in section 3. Section 3 contains comprehensive questions that align to the four strategic focus areas described in Figure 1 above, to capture responses from each FATCA partner. Section 4 contains United States' responses to these same questions.

1.2 Current State of Automatic Exchange of Information

1.2.1 Foreign Account Tax Compliance Act and Intergovernmental Agreements

FATCA provides an opportunity to address the current landscape of information exchange standards and processes. Under the provisions of FATCA, Foreign Financial Institutions (FFIs) must report certain information to the IRS on their U.S. accounts and on the substantial U.S. owners of certain nonfinancial foreign entities (NFFEs). To encourage compliance, the law requires any withholding agent to withhold 30% of any payments made to a non-compliant FFI of U.S. source passive income or of gross proceeds from the sale or disposition of any property that can produce U.S. source interest or dividends.

Understanding that certain jurisdictions may have legal constraints on the ability of their FFIs to comply with FATCA, the U.S. Treasury developed bilateral model intergovernmental agreements (see footnote 1 above). The intergovernmental agreements (also referred to as "IGAs") establish a framework for the provision of information on U.S. accounts and substantial U.S. owners of certain NFFEs. This intergovernmental approach to FATCA implementation serves to address legal impediments as well as to reduce burdens for FFIs. There are essentially two types of model intergovernmental agreements:

- ***Model 1***, which may be a reciprocal (Model 1A) or nonreciprocal (Model 1B) agreement. Under this model, FFIs report U.S. account holder information to their respective tax authorities, followed by the automatic exchange of such information under existing tax treaties or tax information exchange agreements (TIEAs).

- ***Model 2***, which is a nonreciprocal agreement that provides for direct reporting of U.S. account holder information by FFIs to the IRS. Information reporting to the IRS may be supplemented through additional exchange of information requests by the U.S. Competent Authority to the FATCA Partner Competent Authority.

The Model 1A Agreement contains provisions (in Article 3(8)) regarding confidentiality and the required safeguards and infrastructure that must be in place to ensure timely and accurate exchanges and states that the information exchanged will be kept confidential and used solely for tax purposes, in accordance with the provisions of the treaty/TIEA (see the following page for additional information).[2]

[2] This document is the agreement between the U.S. Government and FATCA Partner Government to Improve International Tax Compliance and Implement FATCA. The Model 1A Agreement can be found at this hyperlink: Reciprocal Model 1A Agreement, Preexisting TIEA or DTC. Further information on the model agreements can be found via this hyperlink: Model Intergovernmental Agreements

Relevance for Enforcing Safeguard Compliance

Model 1A IGA Reciprocal, Preexisting TIEA or DTC; Article 3: Time and Manner of Exchange of Information

7. All information exchanged shall be subject to the confidentiality and other protections provided for in the [Convention/TIEA], including the provisions limiting the use of the information exchanged.

8. Following entry into force of this Agreement, each Competent Authority shall provide written notification to the other Competent Authority when it is satisfied that the jurisdiction of the other Competent Authority has in place (i) appropriate safeguards to ensure that the information received pursuant to this Agreement shall remain confidential and be used solely for tax purposes, and (ii) the infrastructure for an effective exchange relationship (including established processes for ensuring timely, accurate, and confidential information exchanges, effective and reliable communications, and demonstrated capabilities to promptly resolve questions and concerns about exchanges or requests for exchanges and to administer the provisions of Article 5 of this Agreement). The Competent Authorities shall endeavor in good faith to meet, prior to September 2015, to establish that each jurisdiction has such safeguards and infrastructure in place.

9. The obligations of the Parties to obtain and exchange information under Article 2 of this Agreement shall take effect on the date of the later of the written notifications described in paragraph 8 of this Article. Notwithstanding the foregoing, if the [FATCA Partner] Competent Authority is satisfied that the United States has the safeguards and infrastructure described in paragraph 8 of this Article in place, but additional time is necessary for the U.S. Competent Authority to establish that [FATCA Partner] has such safeguards and infrastructure in place, the obligation of [FATCA Partner] to obtain and exchange information under Article 2 of this Agreement shall take effect on the date of the written notification provided by the [FATCA Partner] Competent Authority to the U.S. Competent Authority pursuant to paragraph 8 of this Article.

The United States intends to use this International Data Safeguards & Infrastructure Workbook to collect information necessary to perform an initial review of each prospective FATCA Partner's ability to safeguard and exchange information. The IGA includes a good faith commitment that the United States and each FATCA Partner's Competent Authority will work diligently to confirm that the necessary safeguards and infrastructure are in place prior to initiating the automatic exchange of information required by the IGA.

1.2.2 Tax Treaties, Tax Information Exchange Agreements (TIEAs), and Other Bilateral Agreements for the Exchange of Information

The United States has constructed an expansive network of international agreements, including income tax treaties and TIEAs (collectively referred to as information exchange agreements), that provide for the exchange of tax-related information under appropriate circumstances. These information exchange agreements are based on bilateral cooperation and are feasible only if each tax administration is assured that the other tax administration will protect the confidentiality

of information received and limit its use to the purposes permitted under the exchange agreement. Before entering into or revising an information exchange agreement, the United States reviews (in collaboration with its prospective exchange partner) the jurisdiction's laws and practices related to safeguarding exchanged information. In addition, the United States monitors the use of information it provides to another jurisdiction under an information exchange agreement and takes steps to address circumstances in which information is disclosed or used improperly.

In reciprocal IGA instances, the United States' willingness to provide tax information to another jurisdiction depends, in part, on the jurisdiction's commitment and ability to keep information it receives confidential and to ensure that the information will be used exclusively for tax purposes. Such commitments and capabilities are especially critical when information is to be exchanged automatically and "in bulk," even when data is not being exchanged as the result of a specific tax investigation. Before providing tax information to another jurisdiction on an automatic basis, the IRS must carefully evaluate the partner jurisdiction's policies, procedures, and history with respect to safeguarding tax information. Regarding the latter, the IRS will consider its own exchange history with the relevant jurisdiction, including its experience with failures by that jurisdiction to ensure appropriate limitations on the use of exchanged information. The IRS will also verify previous exchange experiences of other U.S. agencies and other jurisdictions that have exchange of information relationships with the prospective partner.

1.2.3 Current OECD Safeguard Standards [3]

The 2012 Joint OECD/Global Forum "Keeping it Safe" Guide sets out best practices related to taxpayer confidentiality and provides practical guidance, including recommendations and a checklist, on how to meet an adequate level of protection when exchanging data electronically. The number of exchange of information agreements has increased dramatically in recent years, and taxpayers and tax administrations have a legal right to expect that data exchanged under exchange of information agreements remains confidential. This requires all partners to maintain adequate safeguards to protect the confidentiality of shared information and provide assurance that information will only be used for the purposes permitted under the exchange of information agreement.

While the first step is ensuring that appropriate legislation is in place, the confidentiality of taxpayer information also depends on the ability to sustain a culture of information security within a tax administration. Confidentiality measures must therefore be incorporated into all tax administration operational aspects. The "Keeping It Safe" report provides general guidance and recommendations on how tax administrations should protect the confidentiality of taxpayer

[3] The 2012 Joint OECD/Global Forum "Keeping it Safe" Guide examines the legal framework to protect the confidentiality of information exchanged and the administrative policies and practices in place to protect confidentiality. Further information can be found via this hyperlink: 2012 Joint OECD/Global Forum Keeping it Safe Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes

information, both domestically and with regard to information exchanged under exchange of information agreements.

1.2.4 Global Forum Peer Review Process [4]

The Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) is an international body that is charged with in-depth monitoring and peer reviews to ensure the implementation of internationally agreed standards of transparency and exchange of information. These standards are primarily reflected in the 2002 OECD Model *Agreement on Exchange of Information on Tax Matters* and its commentary; and in Article 26 of the 2010 OECD *Model Tax Convention on Income and on Capital*.[5] The standards have also been incorporated into the UN *Model Tax Convention*.[6]

The Global Forum was restructured in 2009 and now has 120 member countries. All members of the Global Forum, as well as jurisdictions identified by the Global Forum as relevant to its work, are currently being (or have recently been) reviewed. This process is undertaken in two phases, which may be combined. Phase 1 Reviews assess the quality of a jurisdiction's legal and regulatory framework for the exchange of information, while Phase 2 Reviews assess the practical implementation of that framework. The Global Forum Terms of Reference focus on the exchange of information upon request and rely on the OECD Model Tax Convention Article 26 and the OECD Model Agreement on Exchange of Information (among other international sources) as references for establishing the standards upon which jurisdictions are evaluated.

1.2.5 G20 Meeting of Finance Ministers and Central Bank Governors

On July 19-20, 2013, the communiqué of the G20 meeting of Finance Ministers and Central Bank Governors in Moscow fully endorsed the OECD proposal for a truly global model for multilateral and bilateral automatic exchange of information and committed to automatic exchange of information as the new global standard.[7] The United States Treasury and IRS are

[4] The Global Forum has 121 members (including the European Union) and is the premier international body for ensuring the implementation of international agreed upon standards surrounding transparency and tax exchange of information. Further information can be found via this hyperlink: OECD Global Forum on Tax Transparency

[5] The OECD Model Agreement represents the standard of effective exchange of information for the purposes of the OECD's initiative on harmful tax practices. Further information can be found via this hyperlink: OECD Model Agreement on Exchange of Information on Tax Matters. The OECD Model Tax Convention on Income and on Capital provides a means to settle, on a uniform basis, the most common problems that arise in the field of international juridical double taxation. Further information can be found via hyperlink: OECD Model Tax Convention on Income and on Capital

[6] The UN Model Double Taxation Convention provides a detailed overview of a series of model bilateral tax conventions. Further information can be found via this hyperlink: UN Model Double Taxation Convention

[7] This proposal, prepared at the request of the G20, provided ministers with a proposal to increase international tax cooperation and transparency through the promotion of automatic exchange of information between jurisdictions. Further information can be found via this hyperlink: OECD G20 Statement

fully committed to the automatic exchange of information as the new global standard, and they are dedicated to making the automatic exchange of information attainable by all countries and will seek to provide capacity building support with assistance from the Global Forum. In 2013, the Global Forum established an Automatic Exchange of Information Group, to assist and prepare countries as they move towards implementation of automatic exchange.

1.3 Terms and Definitions

1.3.1 What is Automatic Exchange of Information? [8]

OECD Automatic Exchange of Information Definition

Automatic exchange of information involves the systematic and periodic transmission of "bulk" taxpayer information by the source country to the residence country concerning various categories of income (e.g. dividends, interest, royalties, salaries, pensions, etc.). It can provide timely information on non-compliance where tax has been evaded either on an investment return or the underlying capital sum even where tax administrations have had no previous indications of non-compliance.

The OECD has developed a standardized, secure, and cost effective model for bilateral automatic exchange.[9] A standardized multilateral automatic exchange model requires a legal basis for the exchange of information. There are different legal bases upon which automatic exchange can occur, including a bilateral treaty (see Article 26 of the OECD Model Tax Convention), a TIEA, or the Multilateral Convention on Mutual Administrative Assistance in Tax Matters.

The IRS and U.S. Treasury Department have been collaborating with the OECD to develop a globally agreed upon electronic format for collecting information (schema) with regard to accounts held in financial institutions and a secure transmission method for bulk data exchanged on a regular, recurring basis. The transmission method needs to ensure that the data transmitted on an automatic basis is appropriately safeguarded and that only the intended recipient can have access to the data. In addition, the IRS and U.S. Treasury Department are currently working with the Global Forum to establish a mechanism to monitor and review the implementation of the global standard of automatic exchange of information. The objective is to be able to rely upon a globally agreed process to ensure that data safeguarding systems and practices are (and continue to be) in place and fully functioning.

The IRS will not enter into a new automatic exchange relationship with a jurisdiction unless it has reviewed the jurisdiction's legal framework, policies, and practices and has determined that

[8] This OECD briefing provides an overview of automatic exchange of information, as part of a broader web portal. Further information can be found via this hyperlink: OECD Automatic Exchange of Information Overview

[9] The OECD delivered a single global standard on automatic exchange of information on February 13, 2014: Standard for Automatic Exchange of Financial Account Information

such an exchange relationship is appropriate. Furthermore, the IRS generally will not enter into an automatic exchange relationship unless the other jurisdiction is willing and able to reciprocate effectively. Internal Revenue Code § 6103 and § 6105, which support this notion, are described below. [10]

Internal Revenue Service Code § 6103 and § 6105 - Key Points

§ 6103(k)(4) – A 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 a convention or bilateral agreement.

§ 6103(p) – Accounting for disclosures requires the set-up of a record keeping system and accounting for certain disclosures (Form 5466-B).

Disclosures under § 6103(k)(4) are not exempt from the application of § 6103(p).

§ 6105(a) – Tax convention information is confidential and may not be disclosed unless an exception applies.

1.3.2 What are Other Types of Exchange of Information Processes? [11]

In addition to automatic exchange of information, data may also be exchanged on request or spontaneously. An *exchange of information on request* refers to a situation where the Competent Authority of one jurisdiction asks for particular information from the Competent Authority of another jurisdiction under the provisions of a tax treaty/TIEA. For example, when the IRS receives a request for information, it will evaluate the requesting jurisdiction's current practices with respect to information confidentiality. Additionally, the IRS will require the requesting jurisdiction to explain the intended use of the information and to justify the relevance of that information to the permitted use. *A spontaneous exchange* allows for information to be exchanged extemporaneously when one contracting party—having obtained information in the course of administering its own tax laws—determines that such information may be of interest to a treaty partner for tax purposes, and provides that information to the treaty partner without the necessity of the treaty partner making a request for the information.

[10] Internal Revenue Code (IRC) § 6103 provides rules for the confidentiality and disclosure of returns and return information. Further information can be found via this hyperlink: U.S. Internal Revenue Code (IRC) § 6103 ; and IRC § 6105 provides the rules for confidentiality of information arising under treaty obligations. Further information can be found via this hyperlink: U.S. Internal Revenue Code (IRC) § 6105

[11] The OECD Manual on the Implementation of Exchange of Information for Tax Purposes provides an overview of the operation of exchange of information provisions and technical/practical guidance to improve the efficiency of such exchanges. Further information can be found via this hyperlink: OECD Manual on the Implementation of Exchange of Information Provisions for Tax Purposes

1.3.3 What is Confidentiality and How Does it Apply to Automatic Exchange of Information? [12]

Effective mutual assistance between Competent Authorities requires that each Competent Authority be assured that the other will treat with proper confidentiality the information that it obtains in the course of their cooperation. For this reason, treaties and exchange of information instruments contain provisions regarding confidentiality, and the obligation to keep information exchanged as secret. Information exchange partners may suspend the exchange of information if appropriate safeguards are not in place, if there has been a breach in confidentiality, and/or if they are not satisfied that such situations have been adequately addressed and resolved.

For purposes of the automatic exchange of information, confidentiality is defined across three international tax conventions: Article 26 of the OECD *Model Tax Convention;* Article 8 of the OECD Model *Agreement on Exchange of Information on Tax Matters;* and Article 22 of the OECD *Multilateral Convention on Mutual Administrative Assistance in Tax Matters.*

The key points of the confidentiality provisions in these documents are:

- Confidentiality covers both information provided in a request and information received in response to a request
- Treaty provisions and domestic laws apply to ensure confidentiality
- Information exchanged may only be used for certain specified purposes
- Information exchanged may only be disclosed to certain specified persons

OECD Model Tax Convention, Article 26(2)

Any information received under paragraph 1 by a Contracting State shall be treated as secret in the same manner as information obtained under domestic laws of that State and be disclosed only to persons or authorities (including courts and administrative bodies) concerned with the assessment or collection of, the enforcement or prosecution in respect of, the determination of appeals in relation to the taxes referred to in paragraph 1, or the oversight of the above. Such persons or authorities shall use information only for such purposes, and may disclose information in public court proceedings or in judicial decisions.

Article 26 further outlines the confidentiality rules under the OECD Model Tax Convention, the purposes for which the information may be used, and the limits on to whom the information may be disclosed.

[12] The OECD "Keeping It Safe" report sets out best practices related to confidentiality and provides guidance to protect the confidentiality of taxpayer information both domestically and internationally, specifically with regard to exchange of information instruments. Further information can be found via this hyperlink: OECD Keeping it Safe - Joint OECD/Global Forum Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes

In the Commentary to Article 26 of the OECD Model Tax Convention, disclosure of treaty exchanged taxpayer information is limited to:

- Persons or authorities (including courts and administrative bodies) involved in the assessment, collection, enforcement, prosecution, and determination of appeals of a covered tax
- The taxpayer, his proxy, or a witness
- Governmental or judicial authorities charged with deciding whether such information should be released to the taxpayer, his proxy, or the witnesses
- Oversight bodies
- Third-party jurisdictions, only if there is an express provision in the bilateral treaty allowing such disclosure

Regarding third-party jurisdictions, courts and administrative bodies involved for tax purposes may disclose the information in court sessions or court decisions. Once information becomes public in this way, that information can be used for other purposes by, for example, quoting from the public court files or decisions. The confidentiality rules cover Competent Authority letters, including the letter requesting information. It is understood that the requesting State can disclose the minimum information contained in a Competent Authority letter necessary to obtain or provide the requested information, but may not disclose the letter itself.[13]

Information shall only be used for the above purposes, in accordance with the provisions of the information exchange agreement. It may not be used for other (non-tax) purposes unless otherwise specified in the treaty. In this respect, jurisdictions may include a provision that allows the sharing of information with other law enforcement agencies, provided that there is a Mutual Legal Assistance Treaty (MLAT) in force between the parties that allows for the use of such information for other purposes under the laws of both jurisdictions and the supplying jurisdiction has provided written consent authorizing such use.

[13] The OECD "Keeping It Safe" report examines the legal framework to protect the tax confidentiality of information exchanged and the administrative policies and practices in place to protect confidentiality. Further information can be found via this hyperlink: OECD Keeping It Safe - Joint OECD/Global Forum Guide on the Protection of Confidentiality of Information Exchange for Tax Purposes

OECD Model Agreement on Exchange of Information on Tax Matters, Article 8

Any information received by a Contracting Party under this Agreement shall be treated as confidential and may be disclosed only to persons or authorities (including courts and administrative bodies) in the jurisdiction of the Contracting Party concerned with the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, the taxes covered by this Agreement. Such persons or authorities shall use such information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions. The information may not be disclosed to any other person or entity or authority or any other jurisdiction without the written consent of the competent authority of the requested Party.

Article 8 of the OECD Model TIEA above is similar to Article 26 of the OECD Model Tax Convention, in that they both require that information be kept confidential and be disclosed only to certain persons and used for tax administration purposes. The OECD Model Tax Convention contains the additional requirement that information should be treated "as secret in the same manner as information obtained under the domestic laws of [the requesting] State." In addition, the OECD Model Tax Convention permits disclosure to oversight authorities. The OECD Model TIEA expressly permits disclosure to any other person, entity, authority or jurisdiction provided express written consent is given by the competent authority of the requested party. However, because both the Model TIEA and the Model Tax Convention specify to whom the information can be disclosed and for what purposes the information may be used (thus ensuring a minimum standard of confidentiality), there should be little practical difference between the two formulations.

Multilateral Convention on Mutual Administrative Assistance in Tax Matters, Article 22

1. Any information obtained by a Party under this Convention shall be treated as secret and protected in the same manner as information obtained under the domestic law of that Party and, to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Party as required under its domestic law.
2. Such information shall in any case be disclosed only to persons or authorities (including courts and administrative or supervisory bodies) concerned with the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, taxes of that Party, or the oversight of the above. Only the persons or authorities mentioned above may use the information and then only for such purposes. They may, notwithstanding the provisions of paragraph 1, disclose it in public court proceedings or in judicial decisions relating to such taxes.

The Multilateral Convention is similar to both the OECD Model Tax Convention and the OECD Model TIEA, stating that information be kept confidential. Similar to the Model Tax Convention, the Multilateral Convention specifically references domestic law and allows disclosure to supervisory bodies. Similar to the Model TIEA, the Multilateral Convention permits the

information to be used for other purposes where such use is authorized by the requested party. The Multilateral Convention differs in that it makes specific reference to the protection of personal data, but it supports the notion that information be kept confidential and disclosed only to certain persons and used for certain purposes, similar to the instruments noted above.

1.3.4 What Does Safeguarding Mean as it Relates to Automatic Exchange of information? [14]

U.S. Treasury Publication 4557, Safeguarding Taxpayer Data, Definition

Protective measures prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

U.S. Treasury Publication 1075 Safeguarding Taxpayer Data Definition

Protective measures prescribed to enforce the security requirements specified for an information system, synonymous with security controls and countermeasures. Under the Treasury Publication 1075 guidelines, as a condition of receiving Federal Tax Return and Return Information, the receiving agency must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Enterprise security policies shall address the purpose, scope, responsibilities, and management commitment to implement associated controls, with established safeguards to prevent unauthorized access and use.

A growing number of laws, regulations, standards, and best practices provide guidelines on establishing safeguards that help:

- Preserve the confidentiality and privacy of taxpayer data by restricting access and disclosure;
- Protect the integrity of taxpayer data by preventing improper or unauthorized modification or destruction; and
- Maintain the availability of taxpayer data by providing timely and reliable access and data recovery.

[14] Publication 4557 provides guidance to non-governmental businesses, organizations, and individuals that handle taxpayer data to help them understand and meet their responsibility to safeguard confidential information. Further information can be found via this hyperlink: United States Treasury Publication 4557 - Safeguarding Taxpayer Data; and Publication 1075 provides guidance to ensure that the policies, practices, controls, and safeguards employed by recipient agencies or agents and contractors adequately protect the confidentiality of information received from the IRS. Further information can be found via this hyperlink: United States Treasury Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies

2. EVALUATION PROCESS OVERVIEW

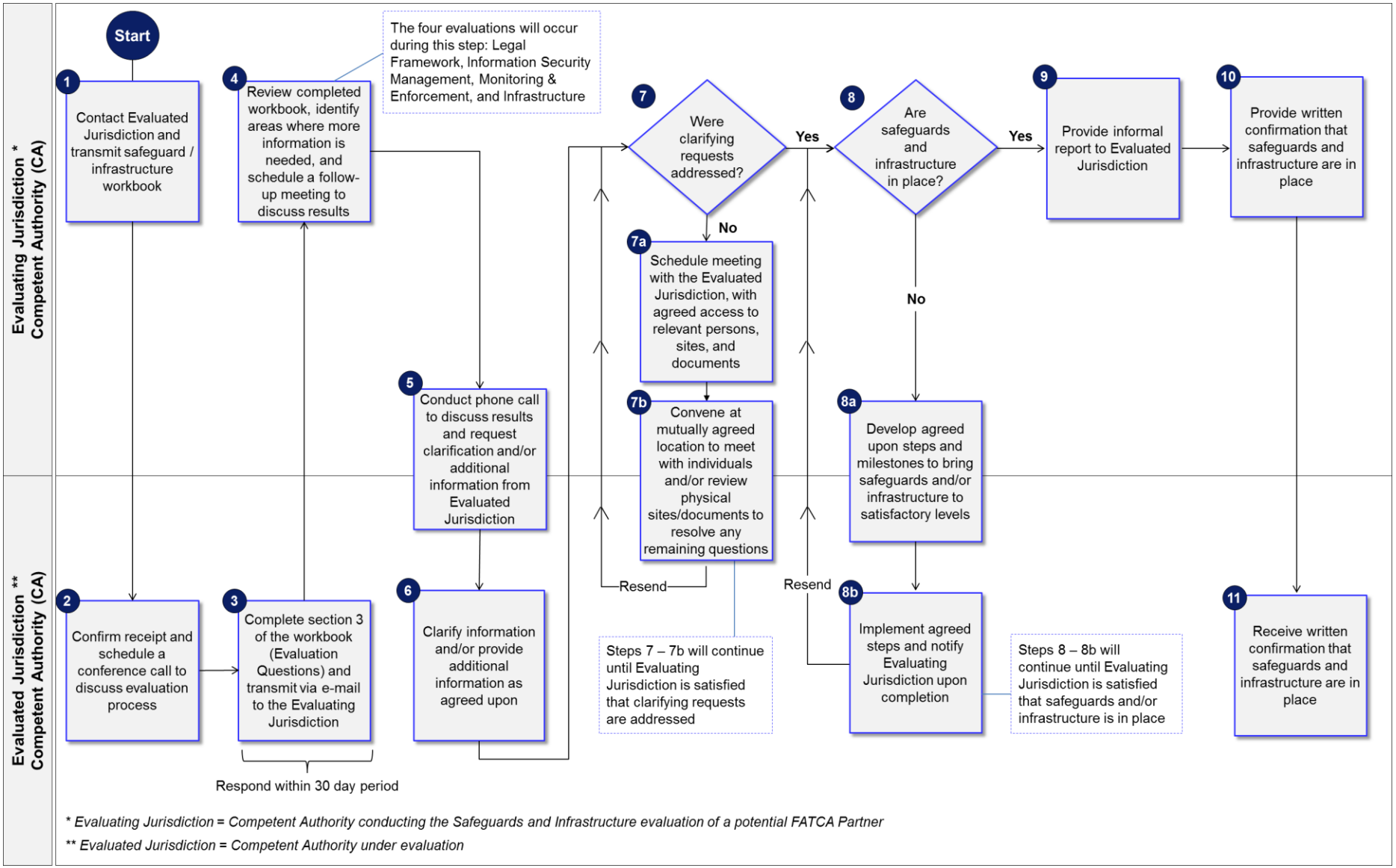
2.1 Scope of Evaluations

The Evaluating Jurisdiction should conduct a comprehensive evaluation of a potential FATCA Partner's safeguard policies and procedures. To complete this process, the Evaluating Jurisdiction will conduct reviews surrounding four primary focus areas: Legal Framework, Information Security Management, Monitoring & Enforcement, and Infrastructure. Confirmation of appropriate security controls will be based on a review of the size, complexity, nature, and scope of exchange of information activities. This may also include the confirmation of policies and records of service providers, ensuring that outside parties maintain an adequate level of information protection defined by the jurisdiction's safeguard practices. Due diligence processes will include: verifying action plans and processes for dealing with automatic exchange, discussing vulnerabilities (theft, disclosure, disruption, unauthorized alterations, and unrecoverable loss), reviewing previous experiences with the Evaluated Jurisdiction, and assessing the Evaluated Jurisdiction's ability to identify and mitigate exchange risks when they arise.

Following receipt of the completed International Data Safeguards & Infrastructure Workbook, the Evaluating Jurisdiction will review available information to identify any potential risks or deficiencies, and will communicate with the Evaluated Jurisdiction to initiate additional information requests, as necessary, and to arrange for an on-site meeting and in-person discussions. The duration of the on-site meeting will depend largely on the Evaluating Jurisdiction's preliminary assessment of the Evaluated Jurisdiction's responses to the questions in Section 3 of this Workbook. It is expected that both the Evaluating Jurisdiction and the Evaluated Jurisdiction will ensure that their respective personnel attending the on-site meeting and participating in the in-person discussions will have the necessary expertise to be able to engage in meaningful discussions on all four of the strategic focus areas described in Section 2.2 of this Workbook.

Based on the outcome of these discussions, the Evaluating Jurisdiction may set forth recommendations for improvement and an associated timeline to modify automatic exchange of information procedures, as determined to be necessary. At any phase during the review process, the Evaluating Jurisdiction may determine that no further work is needed to confirm that automatic exchange of information processes are satisfactory. Upon determining that safeguards and infrastructure are in place, the Evaluating Jurisdiction will provide the Evaluated Jurisdiction with an informal confirmation of such determination, and will commit to providing written confirmation as soon as practicable.

Figure 2 - High-Level Safeguard Evaluation Process Overview



** Evaluating Jurisdiction = Competent Authority conducting the Safeguards and Infrastructure evaluation of a potential FATCA Partner*

*** Evaluated Jurisdiction = Competent Authority under evaluation*

High-Level Safeguard and Infrastructure Evaluation Process Overview

Description
This process flow highlights the steps that an Evaluating Jurisdiction Competent Authority will follow to ensure safeguards and infrastructure are in place in the Evaluated Jurisdiction.

Process Outline		
Step	**Action**	**Detail [Required Documents]**
1	Evaluating Jurisdiction contacts Evaluated Jurisdiction and transmits the International Data Safeguards & Infrastructure Workbook.	▪ The Evaluating Jurisdiction CA transmits formal request to the Evaluated Jurisdiction CA to initiate the process. The initial contact may be an e-mail of introduction followed by a formal transmission of the Workbook via e-mail [Introduction Email and Workbook].
2	Evaluated Jurisdiction confirms receipt and schedules a conference call to discuss process.	▪ The Evaluated Jurisdiction's CA agrees to initiate the process and schedules a discussion to review the Workbook / establish expectations and timeframes [Workbook as a guide to the discussion].
3	Evaluated Jurisdiction completes Workbook and transmits via e-mail to the Evaluating Jurisdiction.	▪ The Evaluated Jurisdiction completes the Workbook and transmits via e-mail to the Evaluating Jurisdiction within 30 day period [Completed Workbook].
4	Evaluating Jurisdiction reviews the completed Workbook and identifies areas where further information and/or discussion is necessary.	▪ The Evaluating Jurisdiction reviews the Evaluated Jurisdiction's completed Workbook and identifies areas where explanations may be unclear and/or an element of safeguards and infrastructure is not in place. Evaluating Jurisdiction schedules a follow-up call to discuss results of their completed Workbook [Completed Workbook].
5	Evaluating Jurisdiction discusses responses, and if necessary, Evaluated Jurisdiction clarifies information and agrees to provide additional information to Evaluating Jurisdiction.	▪ A call is conducted to discuss the Evaluating Jurisdiction's review as well as any questions or the need for additional documentation. Evaluated Jurisdiction provides further explanation, and where necessary, agrees to provide additional information and/or documentation [No Documents].
6	Evaluated Jurisdiction clarifies information and provides any additional information to the Evaluating Jurisdiction as agreed upon.	▪ If necessary, the Evaluated Jurisdiction provides the Evaluating Jurisdiction with additional information to resolve remaining questions [Additional documentation as requested from Evaluating Jurisdiction].
7	Evaluating Jurisdiction reviews responses to clarification requests and additional documentation, and determines if more information is needed. If necessary, additional information is requested and/or a call is scheduled.	▪ The Evaluating Jurisdiction reviews the Evaluated Jurisdiction's additional information and notes areas where the explanations continue to be unclear and/or where there may be a risk that safeguards and infrastructure are not in place. A call is scheduled to discuss the Evaluating Jurisdiction's review as well as any questions / need for additional documentation [Additional information if warranted].

Step	Action	Detail [Required Documents]
7a	Evaluating Jurisdiction schedules a meeting with the Evaluated Jurisdiction. The meeting schedule includes agreed access to relevant persons, sites, and documents.	▪ The Evaluating Jurisdiction schedules a meeting and coordinates with relevant stakeholders to review sites and documentation with the Evaluated Jurisdiction. The meeting will be held in the Evaluated Jurisdiction. [No Documents].
7b	Evaluating Jurisdiction meets with Evaluated Jurisdiction at a mutually agreed location. Meetings occur with individuals to review physical sites and/or documentation to resolve any remaining questions.	▪ The Evaluating Jurisdiction uses the meeting to determine whether the appropriate culture of care exists to prevent the misuse of confidential data and prohibit the inappropriate transfer of tax information. The meeting helps resolve remaining concerns regarding the Evaluated Jurisdiction's safeguards and infrastructure. Activities are conducted and decisions are made as to whether safeguards and infrastructure are in place. (Process returns to step 7; process continues until the Evaluating Jurisdiction is satisfied that clarifying requests are addressed). [Meeting Materials].
8	Evaluating Jurisdiction determines if safeguards / infrastructure are in place. If yes, an informal oral report is made to Evaluated Jurisdiction (see step 9). If no, agreed upon steps are developed with milestones to bring safeguards and/or infrastructure to satisfactory levels (see step 8a).	▪ The Evaluating Jurisdiction will provide an oral report to the Evaluated Jurisdiction regarding the results of their follow-up meeting. If the Evaluating Jurisdiction is satisfied that safeguards and infrastructure are in place, they will report this satisfactory outcome and commit to a written confirmation as soon as practicable. If the Evaluating Jurisdiction is uncertain and requires additional consultation, they will develop steps to bring the Evaluated Jurisdiction to satisfactory levels [No Documents].
8a	Evaluating and Evaluated Jurisdictions develop steps with milestones to bring safeguards and/or infrastructure to satisfactory levels.	▪ The Evaluated Jurisdiction will commit to complete any necessary documentation and/or modify procedures to bring safeguards and/or infrastructure to satisfactory levels [Safeguards Evaluation Report].
8b	Evaluated Jurisdiction takes action to implement agreed steps and notifies Evaluating Jurisdiction when complete.	▪ The Evaluated Jurisdiction will take agreed actions to resolve concerns. Upon completion, the Evaluated Jurisdiction will notify the Evaluating Jurisdiction [Notification may be via e-mail or formal letter]. (Process returns to step 8, and continues until the Evaluating Jurisdiction is satisfied that safeguards and infrastructure are in place).
9	Evaluating Jurisdiction provides informal report to Evaluated Jurisdiction that safeguards and infrastructure are at satisfactory levels.	▪ When the Evaluating Jurisdiction is satisfied that safeguards and infrastructure are in place, it will informally report this satisfactory outcome to the Evaluated Jurisdiction and commit to a written confirmation as soon as practicable.
10	Once satisfied that safeguards and infrastructure are in place, Evaluating Jurisdiction shall provide Evaluated Jurisdiction written confirmation.	▪ The Evaluating Jurisdiction provides formal written confirmation when satisfied that safeguards and infrastructure are in place [Formal Letter].
11	Evaluated Jurisdiction receives confirmation that safeguards and infrastructure are in place.	▪ The Evaluated Jurisdiction receives formal letter to begin automatic exchange.

2.2 Safeguards and Infrastructure Strategic Focus Areas

This section highlights all terms under the four strategic focus areas: Legal Framework, Information Security Management, Monitoring & Enforcement, and Infrastructure. There is a hyperlink for each term, associated with the corresponding question in Section 3 of this Workbook.

2.2.1 Legal Framework Overview

A legal framework must ensure the confidentiality of exchanged tax information and limit its use to appropriate purposes in accordance with the terms of the treaty/TIEA. The two basic components of such a framework are the terms of the applicable treaty, TIEA, or other bilateral agreement for the exchange of information, and a jurisdiction's domestic legislation.

2.2.1.1 Tax Conventions, TIEAs & Other Exchange Agreements

All bilateral and multilateral tax conventions, TIEAs, and other agreements under which tax information is exchanged must contain provisions requiring that the confidentiality of exchanged information be maintained and that its use be limited for certain purposes. The U.S. and the OECD Model Tax Conventions are illustrative. Both require, in Article 26(2), that taxpayer information received by a Competent Authority be treated as secret in the same manner as taxpayer information obtained under the jurisdiction's domestic laws. Both models also restrict disclosure of such information to "persons or authorities (including courts and administrative bodies)" involved in assessment, collection, administration, or enforcement of covered taxes, or in related prosecutions, appeals or oversight. The OECD Model Tax Convention also allows use for another purpose if authorized by both competent authorities and if the laws of both states permit such use. Further, each of the Model IGAs contains provisions for confidentiality. For example, the Model 1A Agreement contains provisions in Article 3(8) regarding confidentiality and the required safeguards and infrastructure that must be in place to ensure timely and accurate exchanges and states that the information exchanged will be kept confidential and used solely for tax purposes (see Section 1.2.1 of this Workbook). (Question 3.1.1)

2.2.1.2 Domestic Legislation

Domestic legislation must include provisions sufficient to protect the confidentiality of taxpayer information and provide for specific and limited circumstances under which such information can be disclosed and used. Domestic law must also impose significant penalties or sanctions for improper disclosure or use of taxpayer information. Further, domestic law must provide that the jurisdiction's tax conventions (treaties, TIEAs, and other bilateral agreements for the exchange of information) are legally binding, such that the confidentiality obligations in such tax conventions will take precedence over any conflicting domestic laws. In order for such legal protections to be meaningful, procedures must be in place to ensure that exchanged taxpayer information can be used solely for tax purposes (or other specified purposes) and to prevent the disclosure of taxpayer information to persons or governmental authorities that are not engaged in the assessment, collection, administration, or enforcement of covered taxes, or in related prosecutions, appeals or oversight. Additionally, a jurisdiction's domestic law for safeguarding

taxpayer data must apply to taxpayer information received from another government under an exchange agreement. (Question 3.1.2)

2.2.2 Information Security Management Overview

The information security management systems used by each jurisdiction's tax administration must adhere to standards that ensure the protection of confidential taxpayer data. For example, there must be a screening process for employees handling the information, limits on who can access the information, and systems to detect and trace unauthorized disclosures. The internationally accepted standards for information security are known as the "ISO/IEC 27000-series", which are published jointly by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). The series provides best practices on information security management, risks, and controls within the context of an overall information security management system. As described more fully below, a tax administration should be able to document readily that it is compliant with the ISO/IEC 27000-series standards or that it has an equivalent information security framework and that taxpayer information obtained under an exchange agreement is protected under that framework.

2.2.2.1 Background Checks and Contracts

Tax administrations must ensure that individuals in positions of authority and access are trustworthy and meet security criteria. Employees, consultants and others with access to confidential information must be screened for potential security risks. Consultants with access to taxpayer information must be contractually bound by the same obligations as employees to keep taxpayer information confidential. (Question 3.2.1)

2.2.2.2 Training and Awareness

Tax administrations must ensure that employees with access to data are aware of the confidentiality requirements of their positions, the security risks associated with their activities, and applicable laws, policies, and procedures related to security/confidentiality. As long as employees continue to have access to data, annual or more frequent training must continue. (Question 3.2.2)

2.2.2.3 Departure Policies

Procedures must exist for quickly ending access to confidential information for terminated, transferred, or retired employees who no longer need such access. (Question 3.2.3)

2.2.2.4 Physical Security: Access to Premises

Tax administrations must have security measures in place to restrict entry to their premises. Measures often include the presence of security guards, policies against unaccompanied visitors, security passes, or coded entry systems for employees and limits on employee access to areas where sensitive information is located. (Question 3.2.4)

2.2.2.5 Physical Security: Physical Document Storage

Tax administrations must also provide secure storage for confidential documents. Information can be secured in locked storage units or rooms, such as cabinets (whether locked with combinations or keys), safes and strong rooms. Access to combinations and keys must be limited only to those with authority to such access. The security of physical storage cabinets must vary depending on the classification of their contents, and bulk tax data exchanged automatically must have a high security classification. Tax administrations must also ensure this security continues when data is taken to alternate work sites. (Question 3.2.5)

2.2.2.6 Planning

Tax administrations must have a plan to develop, document, update, and implement security for information systems. (Question 3.2.6)

2.2.2.7 Configuration Management

Tax administrations must control and manage the configuration of information systems. To this end, they must develop, document, disseminate, and update relevant security controls. (Question 3.2.7)

2.2.2.8 Access Control

Tax administrations must limit system access to authorized users and devices (including other information systems). Authorized users must be limited to accessing the transactions and functions they are permitted to undertake. (Question 3.2.8)

2.2.2.9 Identification and Authentication

Information systems must have the means to store and authenticate the identities of users and devices that require access to information systems. Information systems must also be capable of identifying an unauthorized user and preventing him or her from accessing confidential information. (Question 3.2.9)

2.2.2.10 Audit and Accountability

Unauthorized users can be held accountable only if their actions are traceable. Therefore, it is essential for tax administrations to create and retain information system audit records for monitoring, analyzing, investigating, and reporting of unlawful, unauthorized, or inappropriate information system activity. (Question 3.2.10)

2.2.2.11 Maintenance

Tax administrations must perform periodic and timely maintenance of systems, and provide effective controls over the tools, techniques, and mechanisms for system maintenance and the personnel that use them. (Question 3.2.11)

2.2.2.12 System and Communications Protection

Tax administrations must monitor, control, and protect communications at external and internal boundaries of information systems. These controls must include procedures to remove residual data, provide transmission confidentiality, and validate cryptography. (Question 3.2.12)

2.2.2.13 System and Information Integrity

Tax administrations must identify, report, and correct information system flaws in a timely manner, providing protection from malicious code and monitoring system security alerts and advisories. (Question 3.2.13)

2.2.2.14 Security Assessments

The tax administration must develop and regularly update a policy for reviewing the processes used to test, validate, and authorize the security controls for protecting data, correcting deficiencies and reducing vulnerabilities. It must also have a policy to review the manner in which information system operations and connections are authorized, and the procedures for monitoring system security controls. (Question 3.2.14)

2.2.2.15 Contingency Planning

Tax administrations must establish and implement plans for emergency response, backup operations, and post-disaster recovery of information systems. (Question 3.2.15)

2.2.2.16 Risk Assessment

A tax administration must assess the potential risk of unauthorized access to taxpayer information, and the risk and magnitude of harm from unauthorized use, disclosure, disruption, modification, or destruction of such information or of the taxpayer information systems. It must update its risk assessment periodically or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system. (Question 3.2.16)

2.2.2.17 Systems and Services Acquisition

Tax administrations must ensure that third-party providers of information systems that are engaged to process, store, and transmit treaty-exchanged information use security controls consistent with the necessary computer security requirements. (Question 3.2.17)

2.2.2.18 Media Protection

Tax administrations must protect information in printed form or on digital media, limit information access to authorized users, and sanitize or destroy digital media before disposal or reuse. (Question 3.2.18)

2.2.2.19 Protection of Treaty-Exchanged Data (formerly Prevention of Data Commingling)

Treaty-exchanged data must always be protected against inadvertent disclosure and must be separated from other information or identifiable as protected treaty-exchanged information. If the treaty-exchanged data is included in a file that includes other data and physical separation is impractical, procedures must be in place to ensure that the entire file is safeguarded and clearly labeled to indicate the inclusion of treaty-exchanged data. The treaty-exchanged information itself also must be clearly labeled. Procedures must be in place to ensure that, before such a file is released to an individual or agency authorized to receive tax information from the tax administration but not authorized to access treaty-exchanged data, all treaty-exchanged data has been removed. If treaty-exchanged data is recorded on electronic media with other data, the electronic media must be protected as if it were entirely treaty-exchanged data. If treaty-exchanged data is transmitted by electronic means, the transmitted files must be clearly designated as treaty-exchanged. If the treaty-exchanged data is stored in a database or files are recorded to a database that includes other electronic data, procedures must be in place to ensure that the entire database is safeguarded and clearly labeled to indicate the inclusion of treaty-exchanged data. Procedures must be in place to ensure that, before access to the database is provided to an individual or agency not authorized to access treaty-exchanged data, all treaty-exchanged data has been deleted from the database (or securely partitioned/protected in a way that prevents the unauthorized individual or agency from accessing that data). (Question 3.2.19)

2.2.2.20 Information Disposal Policies

Tax administrations must have policies requiring data to be destroyed as soon as it is no longer needed and ensuring secure disposal of confidential information. Document shredding, burn boxes, or locked waste bin shredding is appropriate for paper documents, and electronic documents should be deleted when no longer necessary. Confidential information must be removed prior to the disposition of computers and information storage devices. (Question 3.2.20)

2.2.3 Monitoring and Enforcement Overview

In addition to keeping treaty-exchanged information confidential, tax administrations must be able to ensure that its use will be limited to the purposes defined by the applicable information exchange agreement. Thus, compliance with an acceptable information security framework alone is not sufficient to protect treaty-exchanged tax data. In addition, domestic law must impose penalties or sanctions for improper disclosure or use of taxpayer information. To ensure implementation, such laws must be reinforced by adequate administrative resources and procedures.

2.2.3.1 Penalties and Sanctions

To protect against unauthorized disclosure of confidential information, agencies should implement a formal sanctions process for personnel and third-party providers who fail to comply with established information security policies and procedures. Policies should consider both civil and criminal sanctions for unauthorized inspection or disclosure. (Question 3.3.1)

2.2.3.2 Policing Unauthorized Access and Disclosure

In addition to having policies that govern access to confidential information, tax administrations must also have processes to monitor compliance with these policies and detect unauthorized access and disclosure. If this occurs, there must be an investigation followed by the preparation of a report for management. The report must include:

- Recommendations for minimizing the repercussions of the incident;
- An analysis of how to avoid similar incidents in the future;
- Recommendations for any penalties to be imposed on the person(s) responsible for the breach, noting that law enforcement authorities should be involved if intentional disclosure is suspected; and
- Reasons for a high degree of confidence that, once implemented, recommended system changes and penalties will prevent similar future breaches.

Additionally, tax administrations should have a process for review and approval of recommendations for policy and procedural changes to avoid future breaches. The tax administration's investigating authority or senior management must ensure that approved recommendations are implemented. (Question 3.3.2)

2.2.3.3 Sanctions and Prior Experiences

In addition to keeping treaty-exchanged information confidential, tax administrations must be able to ensure that its use will be limited to the purposes defined by the applicable information exchange agreement. Thus, compliance with an acceptable information security framework alone is not sufficient to protect treaty-exchanged tax data. In addition, domestic law must specify penalties or sanctions for improper disclosure or use of taxpayer information, and tax administrations must in fact impose these penalties and sanctions against personnel who violate security policies and procedures to deter others from engaging in similar violations. To ensure implementation, such laws must be reinforced by adequate administrative resources and procedures. (Question 3.3.3)

2.2.4 Infrastructure Overview

In order to have an effective exchange relationship between two IGA jurisdictions, each Competent Authority must feel confident that the other party has the proper infrastructure in place to fulfill its reporting obligations under the IGA (for example, requesting and receiving data from domestic Financial Institutions). To do this, the parties must have established processes in place for ensuring timely, accurate, and confidential information exchanges, effective and reliable communications, and demonstrated capabilities to promptly resolve questions and concerns about exchanges or requests for exchanges. Furthermore, parties must be able to administer the compliance and enforcement provisions of the IGAs. The following examples highlight potential scenarios that require the presence of adequate infrastructure for exchange. (Questions 3.4.1, 3.4.2, 3.4.3, 3.4.4)

Example 1: Resolution of Minor and Administrative Errors

While conducting a preliminary data validation of a reporting file, Jurisdiction A discovers that a Reporting FI from Jurisdiction B has neglected to populate the TIN field for a portion of its reportable accounts. Jurisdiction A's Competent Authority notifies Jurisdiction B's Competent Authority of the error.

Jurisdiction B takes the following steps to resolve the error:

1. Review the notice from Jurisdiction A to ensure a proper understanding of the issue
2. Contact the Reporting FI to explain the problem and request confirmation from the Reporting FI that there was in fact an error or omission
3. If the Reporting FI's submission was incomplete, request that the Reporting FI promptly submit a corrected file, and provide this new file to Jurisdiction A
4. If the Reporting FI's submission was complete, resend the original file to Jurisdiction A and conduct a review to determine the reason for the original loss of data.

Example 2: Resolution of Significant Non-Compliance

While conducting a compliance review, Jurisdiction A discovers that a Reporting FI from Jurisdiction B has consistently failed to report on a number of reportable accounts. Jurisdiction A's Competent Authority notifies Jurisdiction B's Competent Authority of non-compliance and requests resolution.

Jurisdiction B takes the following steps to resolve the non-compliance, in accordance with the provisions of its domestic law:

1. Review the notice from Jurisdiction A to ensure a proper understanding of the issue
2. Contact the Reporting FI to explain the problem and request confirmation from the Reporting FI that there was in fact non-compliance

3. If the Reporting FI does not acknowledge the non-compliance, request an explanation of the due diligence processes that the Reporting FI uses to identify reportable accounts
4. Depending on the severity of the non-compliance, pursue one of the following actions:
    a. Contact the FI via letter or an in-person meeting to discuss the non-compliance; obtain corrected information
    b. Demand records and inspect the FI's records, and if appropriate, conduct a criminal investigation; obtain corrected information
5. Provide Jurisdiction A with the corrected information

3. EVALUATION QUESTIONS

Instructions

This section contains a series of tables that address each of the safeguard evaluation areas detailed in the prior section: Legal Framework, Information Security Management, Monitoring & Enforcement, and Infrastructure. All tables contain a primary checklist for reference purposes; a gray box with relevant questions; and an open box provided to insert a response. The Evaluating Jurisdiction will use the Evaluated Jurisdiction's responses as evidence to evaluate compliance surrounding each of the key focus areas for safeguarding data, and determine whether it would be appropriate to engage in automatic exchange of information. Descriptions for each table can be found in section 2.2 of this document.

Please answer all questions and provide detailed responses that address all parts of the question. When providing your response, please be as specific as possible and reference relevant laws, policies, and procedures [and provide electronic links to source documentation], as requested under each sub-category. All responses should be provided in English and be contained within the open box provided. Please do not attach any source documents or send additional documentation in electronic or hard copy under a separate cover.

3.1 Legal Framework

A legal framework must ensure the confidentiality of exchanged tax information and limit its use to appropriate purposes. The two basic components of such a framework are the terms of the applicable treaty, TIEA, or other bilateral agreement for the exchange of information, and a jurisdiction's domestic legislation.

3.1.1 Tax Conventions, TIEAs & Other Exchange Agreements	
Primary Check-list Areas	▪ Provisions in tax treaties, TIEAs and international agreements requiring confidentiality of exchanged information and restricting use to intended purposes
How do the exchange of information provisions in your Tax Conventions, TIEAs, or other exchange agreements ensure confidentiality and restrict the use of both outgoing information to other Contracting States and incoming information received in response to a request? (Description 2.2.1.1)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: Model Conventions you rely upon and language in your Treaty/TIEA network that is equivalent to the OECD Model Tax Convention Article 26(2). (U.S. response 4.1.1) **Enter response here**	

3.1.2 Domestic Legislation	
Primary Check-list Areas	▪ Domestic law must apply safeguards to taxpayer information exchanged pursuant to a treaty, TIEA or other international agreement, and treat those information exchange agreements as binding, restrict data access and use and impose penalties for violations.
How do your domestic laws and regulations safeguard and restrict the use of information exchanged for tax purposes under Tax Conventions, TIEAs, or other exchange instruments? How does the tax administration prevent the misuse of confidential data and prohibit the transfer of tax information from the tax administrative body to non-tax government bodies? (Description 2.2.1.2)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: domestic legislation and regulations. (U.S. response 4.1.2) **Enter response here**	

3.2 Information Security Management

The information security management systems used by each jurisdiction's tax administration must adhere to standards that ensure the protection of confidential taxpayer data. For example, there must be a screening process for employees handling the information, limits on who can access the information and systems to detect and trace unauthorized disclosures. The internationally accepted standards for information security are known as the "ISO/IEC 27000-series." As described more fully below, a tax administration should be able to document that it is compliant with the ISO/IEC 27000-series standards or that it has an equivalent information security framework and that taxpayer information obtained under an exchange agreement is protected under that framework.

3.2.1 Background Checks and Contracts	
Primary Check-list Areas	▪ Screenings and background investigations for employees and contractors ▪ Hiring process and contracts ▪ Responsible Points of Contact
What procedures govern your tax administration's background investigations for employees and contractors who may have access to, use, or are responsible for protecting data received through exchange of information? Is this information publicly available? If so, please provide the reference. If not, please provide a summary of the procedures. **(Description 2.2.2.1)**	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: policies and procedures in place. (U.S. response 4.2.1) **Enter response here**	

3.2.2 Training and Awareness	
Primary Check-list Areas	▪ Initial training and periodic security awareness training based on roles, security risks, and applicable laws
What training does your tax administration provide to employees and contractors regarding confidential information including data received from partners through the Exchange of Information? Does your tax administration maintain a public version of the requirements? If so, please provide the reference. If not, please provide a summary of the requirement. (Description 2.2.2.2)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of training programs focused on taxpayer data confidentiality and related performance measures. (U.S. response 4.2.2) **Enter response here**	

3.2.3 Departure Policies	
Primary Check-list Areas	▪ Departure policies to terminate access to confidential information
What procedures does your tax administration maintain for terminating access to confidential information for departing employees and consultants? Are the procedures publicly available? If so, please provide the reference. If not, please provide a summary of the procedures. (Description 2.2.2.3)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of termination policies. (U.S. response 4.2.3) **Enter response here**	

3.2.4 Physical Security: Access to Premises	
Primary Check-list Areas	▪ Security measures to restrict entry to premises: security guards, policies, entry access procedures
What procedures does your tax administration maintain to grant employees, consultants, and visitors access to premises where confidential information, paper or electronic, is stored? Are the procedures publicly available? If so, please provide the reference. If not, please provide a summary of the procedures. (Description 2.2.2.4)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of premises policies and procedures. (U.S. response 4.2.4) **Enter response here**	

3.2.5 Physical Security: Physical Document Storage	
Primary Check-list Areas	▪ Secure physical storage for confidential documents: policies and procedures
What procedures does your tax administration maintain for receiving, processing, archiving, retrieving and disposing of hard copies of confidential data received from taxpayers or exchange of information partners? Does your tax administration maintain procedures employees must follow when leaving their workspace at the end of the day? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. **Does your tax administration have a data classification policy? If so, please describe how your document storage procedures differ for data at all classification levels. Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. (Description 2.2.2.5)**	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of physical storage policies and procedures. (U.S. response 4.2.5) **Enter response here**	

3.2.6 Planning	
Primary Check-list Areas	▪ Planning documentation to develop, update, and implement security information systems
What procedures does your tax administration maintain to develop, document, update, and implement security for information systems used to receive, process, archive and retrieve confidential information? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. **What procedures does your tax administration maintain regarding periodic Information Security Plan updates to address changes to the information systems environment, and how are problems and risks identified during the implementation of Information Security Plans resolved? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary.** **(Description 2.2.2.6)**	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of Information Security Plans and implementation procedures. (U.S. response 4.2.6) **Enter response here**	

3.2.7 Configuration Management	
Primary Check-list Areas	▪ Configuration management and security controls
What policies does your tax administration maintain to regulate system configuration and updates? Are the policies publicly available? If yes, please provide the reference. If not, please provide a summary. **(Description 2.2.2.7)**	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: standards/processes in place to develop, document, disseminate, and update relevant security control. (U.S. response 4.2.7) **Enter response here**	

3.2.8 Access Control	
Primary Check-list Areas	▪ Access Control Policies and procedures: authorized personnel and international exchange of information
What policies does your tax administration maintain to limit system access to authorized users and safeguard data during transmission when received and stored? Please describe how your tax administration's access authorization and data transmission policies extend to data received from an exchange of information partner under a treaty, TIEA, or other exchange agreement. Are the policies publicly available? If yes, please provide the reference. If not, please provide a summary. **(Description 2.2.2.8)**	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of access control policies and procedural guides. (U.S. response 4.2.8) **Enter response here**	

3.2.9 Identification and Authentication	
Primary Check-list Areas	▪ Authenticating the identifying users and devices that require access to information systems
What policies and procedures does your tax administration maintain for each information system connected to confidential data? Are the policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary. **What policies and procedures govern the authentication of authorized tax administration users by systems connected to confidential data? Are the policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary.** **(Description 2.2.2.9)**	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: identification and authentication policies for systems containing confidential information. (U.S. response 4.2.9) **Enter response here**	

3.2.10 Audit and Accountability	
Primary Check-list Areas	▪ Traceable electronic actions within systems ▪ System audit procedures: monitoring, analyzing, investigating, and reporting of unlawful/unauthorized use
What policies and procedures does your tax administration maintain to ensure system audits take place that will detect unauthorized access? Are the policies publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.10)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of system audit procedures and guidelines. (U.S. response 4.2.10) **Enter response here**	

3.2.11 Maintenance	
Primary Check-list Areas	▪ Periodic and timely maintenance of systems ▪ Controls over: tools, procedures, and mechanisms for system maintenance and personnel use
What policies govern effective periodic system maintenance by your tax administration? Are these policies publicly available? If so, please provide a reference. If not, please provide a summary. **What procedures govern the resolution of system flaws identified by your tax administration? Are these procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.11)**	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of maintenance procedures and guidelines. (U.S. response 4.2.11) **Enter response here**	

3.2.12 System and Communications Protection	
Primary Check-list Areas	▪ Procedures to monitor, control, and protect communications to and from information systems
What policies and procedures does your tax administration maintain for the electronic transmission and receipt of confidential data. Please describe the security and encryption requirements addressed in these policies. Are these policies publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.12)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: internal policies and procedural guidelines. (U.S. response 4.2.12) **Enter response here**	

3.2.13 System and Information Integrity	
Primary Check-list Areas	▪ Procedures to identify, report, and correct information system flaws in a timely manner ▪ Protection against malicious code and monitoring system security alerts
What procedures does your tax administration maintain to identify, report, and correct information system flaws in a timely manner? Please describe how these procedures provide for the protection of systems against malicious codes causing harm to data integrity. Are these procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.13)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of information systems security procedures and guidelines. (U.S. response 4.2.13) **Enter response here**	

3.2.14 Security Assessments	
Primary Check-list Areas	▪ Processes used to test, validate, and authorize the security controls for protecting data, correcting deficiencies, and reducing vulnerabilities
What policies does your tax administration maintain and regularly update for reviewing the processes used to test, validate, and authorize a security control plan? Is the policy publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.14)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of the information systems certification, accreditation and security assessment policies, and procedural guidelines. (U.S. response 4.2.14) **Enter response here**	

3.2.15 Contingency Planning	
Primary Check-list Areas	▪ Plans for emergency response, backup operations, and post-disaster recovery of information systems
What contingency plans and procedures does your tax administration maintain to reduce the impact of improper disclosure of data or unrecoverable loss of data? Are the plans and procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.15)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of systems contingency plans and procedural guidelines. (U.S. response 4.2.15) **Enter response here**	

3.2.16 Risk Assessment	
Primary Check-list Areas	▪ Potential risk of unauthorized access to taxpayer information ▪ Risk and magnitude of harm from unauthorized use, disclosure, or disruption of the taxpayer information systems ▪ Procedures to update risk assessment methodologies
Does your tax administration conduct risk assessments to identify risks and the potential impact of unauthorized access, use, and disclosure of information, or destruction of information systems? What procedures does your tax administration maintain to update risk assessment methodologies? Are these risk assessments and policies publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.16)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of risk identification mitigation plans, procedures, and guidelines. (U.S. response 4.2.16) **Enter response here**	

3.2.17 Systems and Services Acquisition	
Primary Check-list Areas	▪ Methods and processes to ensure third-party providers of information systems process, store, and transmit confidential information in accordance with computer security requirements
What process does your tax administration maintain to ensure third-party providers are applying appropriate security controls that are consistent with computer security requirements for confidential information? Are the processes publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.17)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: an overview of agreements with third-party information system provider(s) as well as policies and procedures to ensure that third-party providers properly process, store, and transmit confidential information. (U.S. response 4.2.17) **Enter response here**	

3.2.18 Media Protection	
Primary Check-list Areas	▪ Processes to protect information in printed or digital form ▪ Security measures used to limit media information access to authorized users only ▪ Methods for sanitizing or destroying digital media prior to disposal or reuse
What processes does your tax administration maintain to securely store and limit access to confidential information in printed or digital form upon receipt from any source? How does your tax administration securely destroy confidential media information prior to its disposal? Are the processes available publicly? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.18)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of media protection policies and media protection controls. (U.S. response 4.2.18) **Enter response here**	

3.2.19 Protection of Treaty-Exchanged Data (formerly Prevention of Data Commingling)	
Primary Check-list Areas	▪ Procedures to ensure treaty-exchanged files are safeguarded and clearly labeled ▪ Classification methods of treaty-exchanged files
What policies and processes does your tax administration maintain to store confidential information and clearly label it as treaty-exchanged after receipt from foreign Competent Authorities? Are these policies and processes publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.19)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: an overview of classification methods used to clearly label treaty-exchanged files and to limit access to authorized users. (U.S. response 4.2.19) **Enter response here**	

3.2.20 Information Disposal Policies	
Primary Check-list Areas	▪ Procedures for properly disposing paper and electronic files
What procedures does your tax administration maintain for the disposal of confidential information? Do these procedures extend to exchanged information from foreign Competent Authorities? Are the procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.2.20)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of records and information management procedures. (U.S. response 4.2.20) **Enter response here**	

3.3 Monitoring and Enforcement

In addition to keeping treaty-exchanged information confidential, tax administrations must be able to ensure that its use will be limited to purposes defined by the applicable information exchange agreement. Thus, compliance with an acceptable information security framework alone is not sufficient to protect treaty-exchanged tax data. In addition, domestic law must impose penalties or sanctions for improper disclosure or use of taxpayer information. To ensure implementation, laws must be reinforced by adequate administrative resources and procedures.

3.3.1 Penalties and Sanctions	
Primary Check-list Areas	▪ Penalties imposed for unauthorized disclosures ▪ Risk mitigation practices
Does your tax administration have the ability to impose penalties for unauthorized disclosures of confidential information? Do the penalties extend to unauthorized disclosure of confidential information exchanged with a treaty or TIEA partner? Are the penalties publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.3.1)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of confidentiality policies and risk mitigation overviews. (U.S. response 4.3.1) **Enter response here**	

3.3.2 Policing Unauthorized Access and Disclosure	
Primary Check-list Areas	▪ Monitoring to detect breaches ▪ Reporting of breaches
What procedures does your tax administration have to monitor confidentiality breaches? What policies and procedures does your tax administration have that require employees and contractors to report actual or potential breaches of confidentiality? What reports does your tax administration prepare when a breach of confidentiality occurs? Are these policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Description 2.2.3.2)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of mechanisms in place to document breaches of confidentiality and reports for internal/external stakeholders. (U.S. response 4.3.2) **Enter response here**	

3.3.3 Sanctions and Prior Experience	
Primary Check-list Areas	▪ Prior unauthorized disclosures ▪ Policy/process modifications to prevent future breaches
Have there been any cases in your jurisdiction where confidential information has been improperly disclosed? Have there been any cases in your jurisdiction where confidential information received by the Competent Authority from an exchange of information partner has been disclosed other than in accordance with the terms of the instrument under which it was provided? Does your tax administration or Inspector General make available to the public descriptions of any breaches, any penalties/sanctions imposed, and changes put in place to mitigate risk and prevent future breaches? If so, please provide a reference. If not, please provide a summary. **(Description 2.2.3.3)**	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of reports related to unauthorized disclosures of confidential information. (U.S. response 4.3.3) **Enter response here**	

3.4 Infrastructure

In order to have an effective exchange relationship between two IGA jurisdictions, each Competent Authority must feel confident that the other party has the proper infrastructure in place to fulfill its reporting obligations under the IGA (for example, requesting and receiving data from domestic Financial Institutions). To this end, the parties must have established processes for ensuring timely, accurate, and confidential data exchange, reliable communications, and capabilities to promptly resolve questions or concerns about exchange or requests to exchange. Furthermore, parties must be able to administer the compliance and enforcement provisions within the IGAs: Article 5(1) Minor and Administrative Errors and (2) Significant Non-Compliance.

3.4.1 Collection and Transmission of Information from Financial Institutions	
Primary Check-list Areas	▪ Bulk information exchange processes ▪ Information protection
Does your domestic legal framework require bulk reporting of information with respect to residents' or non-residents' income or other direct tax related items? If so, what procedures does your tax administration have that describe the steps to receive/process bulk data for accounts held by Financial Institutions in your jurisdiction? How do these procedures and your information technology systems ensure confidentiality and limit the use of the data received and transmitted? (Description 2.2.4)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of your bulk information exchange procedures and policies to ensure confidentiality and limit use to authorized persons. (U.S. response 4.4.1) **Enter response here**	

3.4.2 Prior Experience with Bulk Exchange	
Primary Check-list Areas	▪ Automatic exchange history ▪ Problem resolution ▪ Process improvements
Have you automatically exchanged bulk information on a recurring basis with treaty or TIEA partners, and have you received any feedback about the quality, usefulness and timeliness of these past exchanges? What modifications, if any, were made in response to feedback from exchange partners, and how successful were the modifications? (Description 2.2.4)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of your bulk data exchange experience, and information on issue resolution related to existing exchange relationships and subsequent process improvements. (U.S. response 4.4.2) **Enter response here**	

3.4.3 Minor and Administrative Errors	
Primary Check-list Areas	▪ Data validation ▪ Error resolution
What is your process for validating information received from taxpayers and Financial Institutions? If your tax administration identifies data quality problems (for example, missing fields or improperly reported amounts), what steps are taken to make inquiries to the Financial Institution to resolve the data quality problems, and can penalties be assessed if these issues are not resolved within a specified period of time? (Description 2.2.4)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of data validation procedures and policies for interacting with taxpayers and information suppliers. (U.S. response 4.4.3) **Enter response here**	

3.4.4 Significant Non-Compliance	
Primary Check-list Areas	▪ Resolution of significant non-compliance ▪ Policies and processes for audits and investigations ▪ Audit history
Does your jurisdiction's legal framework allow for audits of taxpayers, including the ability to demand and receive information from taxpayers and Financial Institutions? Are such audits regularly conducted, and if so, what are the characteristics of audits that have been conducted during the last [3] years? (Description 2.2.4)	
Please provide a detailed description [including links to relevant supporting documentation] that outlines items such as: overview of policies related to information requests, audit policies and procedures, limitations on the scope of audits, and audit program history. (U.S. response 4.4.4) **Enter response here**	

APPENDIX

U.S. RESPONSES TO SAFEGUARDS AND INFRASTRUCTURE QUESTIONS

4.1 Legal Framework

A legal framework must ensure the confidentiality of exchanged tax information and limit its use to appropriate purposes. The two basic components of such a framework are the terms of the applicable treaty, TIEA, or other bilateral agreement for the exchange of information, and a jurisdiction's domestic legislation.

4.1.1 Tax Conventions, TIEAs & Other Exchange Agreements	
Primary Check-list Areas	▪ Provisions in tax treaties, TIEAs, and international agreements requiring confidentiality of exchanged information and restricting use to intended purposes
How do the exchange of information provisions in your Tax Conventions, TIEAs, or other exchange agreements ensure confidentiality and restrict the use of both outgoing information to other Contracting States and incoming information received in response to a request? (Question 3.1.1)	
Information exchange provisions based on Article 26 of the U.S. Model Income Tax Convention and included in most U.S. tax treaties and TIEAs require exchanged information to be kept secret and subjected to the same disclosure constraints as information obtained under the laws of the requesting State. Received information may only be disclosed to and used by courts, administrative bodies and others involved in and for the purposes of assessment, collection, or administration, enforcement or prosecution, or determination of appeals concerning the taxes covered by the agreement. Information may also be disclosed to legislative bodies, such as the tax-writing committees of the U.S. Congress and the U.S. Government Accountability Office, engaged in and solely for use in overseeing tax law administration. Article 26 of the OECD Model Tax Convention is similar, but also allows use of exchanged information for other purposes, as both competent authorities and the laws of both countries permit.	

4.1.2 Domestic Legislation	
Primary Check-list Areas	▪ Domestic law must apply safeguards to taxpayer information exchanged pursuant to a treaty, TIEA, or other international agreement and treat those information exchange agreements as binding, restrict data access and use and impose penalties for violation.
How do your domestic laws and regulations safeguard and restrict the use of information exchanged for tax purposes under Tax Conventions, TIEAs, or other exchange instruments? How does the tax administration prevent the misuse of confidential data and prohibit the transfer of tax information from the tax administrative body to non-tax government bodies? (Question 3.1.2)	
I.R.C. § 6103 requires the IRS to maintain return information as confidential unless a provision of Title 26 (Internal Revenue Code) provides otherwise. "Return information" broadly includes the taxpayer's identity and all other information received, acquired, or generated by the IRS in connection with the determination of a taxpayer's tax liability. See I.R.C. § 6103(b)(2). Returns and return information may be disclosed to the competent authority of a foreign government if the foreign government has an income, estate, or gift tax convention or other convention or bilateral agreement, to the extent provided in such convention or bilateral agreement with the United States. I.R.C. § 6103(k)(4). Additionally, I.R.C. § 6105 generally provides that information exchanged under (and agreements concluded under) a tax convention may not be disclosed. Certain limited exceptions permit disclosure: (1) when permitted under the terms of the relevant treaty or TIEA; (2) in accordance with generally applicable procedural rules regarding applications for relief under the treaty; (3) with the written permission of the treaty or TIEA partner when treaty-exchanged information relates to certain terrorist incidents, threats or activities; and (4) for treaty-exchanged data that does not relate to a particular taxpayer, if the U.S. Competent Authority determines, after consultation with the treaty or TIEA partner, that such disclosure would not impair tax administration.	

4.2 Information Security Management

The information security management systems used by each jurisdiction's tax administration must adhere to standards that ensure the protection of confidential taxpayer data. For example, there must be a screening process for employees handling the information, limits on who can access the information, and systems to detect and trace unauthorized disclosures. The internationally accepted standards for information security is known as the "ISO/IEC 27000-series." As described more fully below, a tax administration should be able to document that it is compliant with the ISO/IEC 27000-series standards or that it has an equivalent information security framework and that taxpayer information obtained under an exchange agreement is protected under that framework.

4.2.1 Background Checks and Contracts	
Primary Check-list Areas	▪ Screenings and background investigations for employees and contractors ▪ Hiring process and contracts ▪ Responsible Points of Contact
What procedures govern your tax administration's background investigations for employees and contractors who may have access to, use, or are responsible for protecting data received through exchange of information? Is this information publicly available? If so, please provide the reference. If not, please provide a summary of the procedures. (Question 3.2.1)	
The IRS has a publicly available procedure that describes screenings and background investigations for employees and contractors. The screenings and background investigations are conducted in accordance with procedures outlined in IRS policy in Internal Revenue Manual (IRM) 10.23.1, Personnel Security; IRM 10.23.2, Contractor Investigations; and IRM 10.23.3, Personnel Security/Suitability Program. (National Institute of Standards and Technology (NIST) SP 800-53 for Physical and Environmental Protection.)	

4.2.2 Training and Awareness	
Primary Check-list Areas	▪ Initial training and periodic security awareness training based on roles, security risks, and applicable laws
What training does your tax administration provide to employees and contractors regarding confidential information including data received from partners through the Exchange of Information? Does your tax administration maintain a public version of the requirements? If so, please provide the reference. If not, please provide a summary of the requirement. (Question 3.2.2)	
The IRS policies related to annual security awareness training and role-based security-related training are outlined in IRM 10.8.1.4.2 and are not publicly available. These policies require all employees, contractors, and interns to receive security awareness training when joining the IRS, when required by information system changes, and annually thereafter. Role-based security training is required for individuals whose responsibilities include security responsibilities.. (NIST SP 800-53 for Awareness and Training.)	

4.2.3 Departure Policies	
Primary Check-list Areas	▪ Departure policies to terminate access to confidential information
What procedures does your tax administration maintain for terminating access to confidential information for departing employees and consultants? Are the procedures publicly available? If so, please provide the reference. If not, please provide a summary of the procedures. (Question 3.2.3)	
The IRS policies addressing employees, contractors, or interns are contained in IRM 10.8.1.4.13.4 (2) and are not publicly available. The IRS implements and maintains procedures to ensure revocation of system access, as appropriate, for employees/contractors who leave the IRS, are reassigned to other duties, are on extended leave, or are under disciplinary actions. (NIST SP 800-53 for Personnel Security.)	

4.2.4 Physical Security: Access to Premises	
Primary Check-list Areas	▪ Security measures to restrict entry to premises: security guards, policies, entry access procedures
What procedures does your tax administration maintain to grant employees, consultants, and visitors access to premises where confidential information, paper or electronic, is stored? Are the procedures publicly available? If so, please provide the reference. If not, please provide a summary of the procedures. (Question 3.2.4)	
The IRS policy is contained in IRM 10.8.1.4.11.1 and is not publicly available. The IRS maintains, disseminates, and reviews a formal, documented physical and environmental protection policy. This includes the use of a list of individuals authorized to access IRS facilities, the enforcement of physical access control measures, visitor welcome and monitoring procedures, and the enforcement of identification tokens.(NIST SP 800-53 for Physical and Environmental Protection.)	

4.2.5 Physical Security: Physical Document Storage	
Primary Check-list Areas	▪ Secure physical storage for confidential documents: policies and procedures
What procedures does your tax administration maintain for receiving, processing, archiving, retrieving and disposing of hard copies of confidential data received from taxpayers or exchange of information partners? Does your tax administration maintain procedures employees must follow when leaving their workspace at the end of the day? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. **Does your tax administration have a data classification policy? If so, please describe how your document storage procedures differ for data at all classification levels. Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. (Question 3.2.5)**	
The IRS policy defined in IRM 10.2.14 implements a publicly-available "Clean Desk Policy" for employees and addresses locked containers, security containers, safes/vaults, restricted areas, secured rooms, and locks (types of locks, other access controls, inspection, and maintenance procedures for locks, and control and safeguarding of keys and cipher lock combinations). Additionally, the non-public policies outlined in IRM 10.8.1.4.10 address media access, marking, storage, transport, sanitation, and use. (NIST SP 800-53 for Physical and Environmental Protection.)	

4.2.6 Planning	
Primary Check-list Areas	▪ Planning documentation to develop, update, and implement security information systems
What procedures does your tax administration maintain to develop, document, update, and implement security for information systems used to receive, process, archive and retrieve confidential information? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. **What procedures does your tax administration maintain regarding periodic Information Security Plan updates to address changes to the information systems environment, and how are problems and risks identified during the implementation of Information Security Plans resolved? Are these procedures publicly available? If yes, please provide the reference. If not, please provide a summary. (Question 3.2.6)**	
The IRS policy in IRM 10.8.1.4.12.1 states that every Federal Information Security Management Act (FISMA) reportable system will have a security plan developed that, at a minimum, is consistent with the IRS's guidance and templates. This policy is not publicly available. This plan is reviewed on a regular basis and updated to address changes to the information system/environment of operation and problems identified during plan implementation or security control assessments. (Based on NIST SP 800-53 for Planning.)	

4.2.7 Configuration Management	
Primary Check-list Areas	▪ Configuration management and security controls
What policies does your tax administration maintain to regulate system configuration and updates? Are the policies publicly available? If yes, please provide the reference. If not, please provide a summary. (Question 3.2.7)	
The IRS policy in IRM 10.8.1.4.5 states that the IRS shall develop, disseminate, review and update every three (3) years (or sooner if there is a significant change) a formal, documented configuration management policy. This policy is not publicly available. It includes the organization of an oversight function, a configuration management procedure, the creation of configuration baselines, and a review process to ensure consistent device configurations throughout the enterprise. This policy must be consistent with applicable federal laws, Executive Orders, Directives, Policies, Regulations, Standards, and Guidance. (NIST SP 800-53 for Configuration Management.)	

4.2.8 Access Control	
Primary Check-list Areas	▪ Access Control Policies and procedures: authorized personnel and international exchange of information
What policies does your tax administration maintain to limit system access to authorized users and safeguard data during transmission when received and stored? Please describe how your tax administration's access authorization and data transmission policies extend to data received from an exchange of information partner under a treaty, TIEA, or other exchange agreement. Are the policies publicly available? If yes, please provide the reference. If not, please provide a summary. (Question 3.2.8)	
The IRS Policy defined in IRM 10.8.1.4.1 requires the IRS to document procedures for facilitating implementation of the Access Control Policy and associated access controls. Logical access control systems use Personal Identity Verification (PIV) credentials. The policy is not publicly available. Authentication with Homeland Security Presidential Directive -12 (HSPD-12) credentials shall be required for access to all systems. All authorized users and their access authorizations shall be identified and documented. (NIST SP 800-53 for Identification and Authentication.) This policy covers access to all systems with confidential information.	

4.2.9 Identification and Authentication	
Primary Check-list Areas	▪ Authenticating the identifying users and devices that require access to information systems
What policies and procedures does your tax administration maintain for each information system connected to confidential data? Are the policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary. **What policies and procedures govern the authentication of authorized tax administration users by systems connected to confidential data? Are the policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.9)**	
The IRS maintains policies and procedures to authenticate and identify users, to record access and use. The policies and procedures are not publicly available. IRM 10.8.1.4.7 requires a separate procedural document for each information system, in accordance with the IRS Identification and Authentication Policy. Information systems must uniquely identify and authenticate users and capture accesses to those systems. (NIST SP 800-53 for Identification and Authentication.)	

4.2.10 Audit and Accountability	
Primary Check-list Areas	▪ Traceable electronic actions within systems ▪ System audit procedures: monitoring, analyzing, investigating, and reporting of unlawful/unauthorized use
What policies and procedures does your tax administration maintain to ensure system audits take place that will detect unauthorized access? Are the policies publicly available? If so, please provide a reference. If not, please provide a summary. **(Question 3.2.10)**	
The IRS maintains policies and procedures to ensure user access and use is audited to detect unauthorized access. The policies and procedures are not publicly available. IRM 10.8.1.4.3 requires the IRS to develop, disseminate, review, and update a formal, documented audit and accountability policy every three (3) years (or when there is a significant change). IRM 10.8.3 provides overall auditing guidance for the IRS with respect to system accesses and use and takes precedence over all other IRMs. (NIST SP 800-53 for Audit and Accountability.)	

4.2.11 Maintenance	
Primary Check-list Areas	▪ Periodic and timely maintenance of systems ▪ Controls over: tools, procedures, and mechanisms for system maintenance and personnel use
What policies govern effective periodic system maintenance by your tax administration? Are these policies publicly available? If so, please provide a reference. If not, please provide a summary. **What procedures govern the resolution of system flaws identified by your tax administration? Are these procedures publicly available? If so, please provide a reference. If not, please provide a summary.** **(Question 3.2.11)**	
The IRS policies for system maintenance are defined in IRM 10.8.1.4.9 and IRM 2.7.1, Information Technology (IT) Operations, Inter-center, which are not publicly available. IRM 2.7.1.6.4 concerning Preventive Maintenance (PM) and Unscheduled Maintenance (UM) provides further guidance. PM is performed as required by a vendor on a scheduled basis to keep equipment in proper operating condition; UM, when equipment failure has occurred. These policies provide for the managed maintenance of information system components in accordance with manufacturer and IRS requirements. They include executive oversight of maintenance operations, sanitization of media prior to removal from IRS facilities, and review of security controls for operational efficiency. (NIST SP 800-53 for Maintenance.)	

4.2.12 System and Communications Protection	
Primary Check-list Areas	▪ Procedures to monitor, control, and protect communications to and from information systems

What policies and procedures does your tax administration maintain for the electronic transmission and receipt of confidential data. Please describe the security and encryption requirements addressed in these policies. Are these policies publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.12)

The IRS policy regarding the protection of data when removed from systems is not publicly available and is found at IRM 10.8.1.4.10.5. Specifically, the section addresses the removal of residual data, requires that both digital and non-digital information system media be sanitized prior to: (i) disposal, (ii) release from organizational control, or (iii) release for reuse. (NIST SP 800-53 for Media Protection.)

The following Policies regarding systems interface, transmission confidentiality and encryption/cryptography are not publicly available. A brief summary follows:

- Policy stated in IRM 10.8.1.4.16.1 requires IRS information systems to separate user functionality (including user interface services) from information system management functionality and to isolate security from non-security functions. (NIST SP 800-53 for System and Communications Protection.)
- IRM 10.8.1.4.16.7 provides policies on transmission confidentiality. (NIST SP 800-53 for System and Communications Protection.)
- IRM 10.8.1.4.16.12 provides policies on encryption/cryptography and details about the kind of cryptography needed and when it should be employed. (NIST SP 800-53 for System and Communications Protection, Media Protection, and Access Control.)

4.2.13 System and Information Integrity	
Primary Check-list Areas	▪ Procedures to identify, report, and correct information system flaws in a timely manner ▪ Protection against malicious code and monitoring system security alerts
What procedures does your tax administration maintain to identify, report, and correct information system flaws in a timely manner? Please describe how these procedures provide for the protection of systems against malicious codes causing harm to data integrity. Are these procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.13)	
The IRS policy and procedures to identify system flaws and remediate timely, and the procedures to protect against malicious codes are outlined in IRM 10.8.1.4.17 and are not publicly available. All enterprise devices must complete a security review prior to connection. The policies also require periodic enterprise review. The IRS provides for the remediation of identified system flaws within a quarantined environment. (NIST SP 800-53 for System and Information Integrity.)	

4.2.14 Security Assessments	
Primary Check-list Areas	▪ Processes to test, validate, and authorize the security controls for protecting data, correcting deficiencies, and reducing vulnerabilities
What policies does your tax administration maintain and regularly update for reviewing the processes used to test, validate, and authorize a security control plan? Is the policy publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.14)	
This IRS policy outlined in IRM 10.8.1.4.4 requires the IRS to manage the security state of organizational information systems through security authorization processes; designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and fully integrate the security authorization processes into an organization-wide risk management program. It is not publicly available. The plan: a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; b. Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and is updated every 3 years. (NIST SP 800-53 for Program Management.)	

4.2.15 Contingency Planning	
Primary Check-list Areas	▪ Plans for emergency response, backup operations, and post-disaster recovery of information systems
What contingency plans and procedures does your tax administration maintain to reduce the impact of improper disclosure or unrecoverable loss of data? Are the plans and procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.15)	
These IRS plans and procedures are outlined in IRM 10.8.1.4.6 and state the IRS shall develop, disseminate, review, and update annually procedures to facilitate the implementation of the Contingency Planning Policy and associated contingency planning controls. These procedures include the development of a contingency plan appropriate to system categorization, coordination with IRS organizational elements, business resumption planning, and testing of the overall contingency approach. These are not publicly available. (NIST SP 800-53 for Contingency Planning.)	

4.2.16 Risk Assessment	
Primary Check-list Areas	▪ Potential risk of unauthorized access to taxpayer information ▪ Risk and magnitude of harm from unauthorized use, disclosure, or disruption of the taxpayer information systems ▪ Procedures to update risk assessment methodologies
Does your tax administration conduct risk assessments to identify risks and the potential impact of unauthorized access, use, and disclosure of information, or destruction of information systems? What procedures does your tax administration maintain to update risk assessment methodologies? Are these risk assessments and policies publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.16)	
These IRS policies and procedures are outlined in IRM 10.8.1.4.14 and require the IRS to develop, disseminate, review, and annually update procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. These policies address the security categorization of IRS information systems, vulnerability and risk assessments, and staff requirements for those interfacing with systems across all categorization levels. They are not publicly available.(NIST SP 800-53 for Risk Assessment.)	

4.2.17 Systems and Services Acquisition	
Primary Check-list Areas	▪ Processes to ensure third-party providers of information systems process, store, and transmit confidential information in accordance with computer security requirements
What process does your tax administration maintain to ensure third-party providers are applying appropriate security controls that are consistent with computer security requirements for confidential information? Are the processes publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.17)	
This IRS policy outlined in IRM 10.8.1.4.15.3 requires that the IRS develop, disseminate, review, and annually update procedures to facilitate the implementation of procedures employed during the acquisition of systems and services. It addresses the determination of system security needs at the infrastructure and software levels, the establishment of a vendor evaluation process, and acquisition oversight and documentation requirements. This policy is not publicly available. (NIST SP 800-53 for System and Services Acquisition.)	

4.2.18 Media Protection	
Primary Check-list Areas	▪ Processes to protect information in printed or digital form ▪ Security measures used to limit media information access to authorized users only ▪ Methods for sanitizing or destroying digital media prior to disposal or reuse
What processes does your tax administration maintain to securely store and limit access to confidential information in printed or digital form upon receipt from any source? How does your tax administration securely destroy confidential media information prior to its disposal? Are the processes available publicly? If so, please provide a reference. If not, please provide a summary. (Question 3.2.18)	
The IRS processes for information protection, access limitations and methods for securely destroying media before disposal are not publicly available. They are summarized below: • IRS policy in IRM 10.8.1.4.10, reflects the IRS annually-updated procedures to facilitate the implementation of the Media Protection Policy and associated media protection controls. (NIST SP 800-53 for Media Protection.) • As specified in IRM 10.8.1.4.10.5(4), procedures shall be established to ensure sensitive information stored on any media (removable or non-removable) in the possession of an individual (employee or contractor) who is terminated or reassigned, is transferred to an authorized individual for sanitization prior to the IT resource's disposal. (NIST SP 800-53 for Media Protection.) • In accordance with IRM 10.8.1.4.10.4(1), the IRS shall protect and control digital (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm) during transport outside of controlled areas; maintain accountability for the chain of custody of information systems during transport outside of controlled areas; and restrict the activities associated with transport of such media to authorized personnel. (NIST SP 800-53 for Media Protection.)	

4.2.19 Protection of Treaty-Exchanged Data (formerly Prevention of Data Commingling)	
Primary Check-list Areas	▪ Procedures to ensure treaty-exchanged files are safeguarded and clearly labeled ▪ Classification methods of treaty-exchanged files
What policies and processes does your tax administration maintain to store confidential information and clearly label it as treaty-exchanged after receipt from foreign Competent Authorities? Are these policies and processes publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.19)	
The IRS has policies and processes to store and label confidential information. These policies and processes are not publicly available. IRS policy is outlined in IRM 10.8.1.4.16.7.3, Trusted Internet Connections (TICs), and any other IRS Internet connections shall implement technical controls to identify and prevent, to the extent possible through commercially available technology, the transmission outside the IRS of (i) unencrypted information, prior to encryption required for such transmission and (ii) information that should not leave IRS whether or not encrypted. Treasury Directive Publication 85-01 S-SDP.6, 7 provides further procedural details. In accordance with IRM 10.8.1.4.1.16, remote access capabilities shall provide strong identification and authentication and shall protect sensitive/classified information throughout transmission. (NIST SP 800-53 for Access Control.) As specified in IRM 10.8.1.4.10.2 (1), all removable information system media and information system output shall be marked in accordance with IRS policies and procedures, indicating the sensitivity, distribution limitations, handling caveats, and applicable security markings (if any) of the information. (NIST SP 800-53 for Media Protection.)	

4.2.20 Information Disposal Policies	
Primary Check-list Areas	▪ Procedures for properly disposing of paper and electronic files
What procedures does your tax administration maintain for the disposal of confidential information? Do these procedures extend to exchanged information from foreign Competent Authorities? Are the procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.2.20)	
The IRS maintains publicly available policy and procedures for disposing of confidential information. IRS policy for records control schedules is defined in IRM 1.15, Records and Information Management. IRS policy and procedures for disposing of paper and electronic files is contained in IRM 1.15.3.	

4.3 Monitoring and Enforcement

In addition to keeping treaty-exchanged information confidential, tax administrations must be able to ensure that its use will be limited to the purposes defined by the applicable information exchange agreement. Thus, compliance with an acceptable information security framework alone is not sufficient to protect treaty-exchanged tax data. In addition, domestic law must impose penalties or sanctions for improper disclosure or use of taxpayer information. To ensure implementation, such laws must be reinforced by adequate administrative resources and procedures.

4.3.1 Penalties and Sanctions	
Primary Check-list Areas	▪ Penalties imposed for unauthorized disclosures ▪ Risk mitigation practices
Does your tax administration have the ability to impose penalties for unauthorized disclosures of confidential information? Do the penalties extend to unauthorized disclosure of confidential information exchanged with a treaty or TIEA partner? Are the penalties publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.3.1)	
The IRS and the Treasury Inspector General for Tax Administration (TIGTA) are able to impose a wide range of penalties for unauthorized access to or unauthorized disclosure of confidential information. Information regarding the penalties that may be imposed is publicly available. There are several components of our legal framework that prohibit wrongful access to confidential information and provide substantial penalties for wrongful access and disclosure of returns and return information, including: • 5 U.S.C. § 552a – Records Maintained on Individuals; • 18 U.S.C. §§ 641, 1905 – Public Money, Property or Records and Disclosure of Confidential Information Generally; • I.R.C. §§ 7213, 7213A, and 7431 apply specifically to the unauthorized access and disclosure of returns and return information.	

4.3.2 Policing Unauthorized Access and Disclosure	
Primary Check-list Areas	▪ Monitoring to detect breaches ▪ Reporting of breaches
What procedures does your tax administration have to monitor confidentiality breaches? What policies and procedures does your tax administration have that require employees and contractors to report actual or potential breaches of confidentiality? What reports does your tax administration prepare when a breach of confidentiality occurs? Are these policies and procedures publicly available? If so, please provide a reference. If not, please provide a summary. (Question 3.3.2)	
The IRS has procedures in place to monitor breaches of confidentiality, to require employees and contractors to report breaches of confidentiality and to prepare reports of any breach of confidentiality. These policies and procedures are publicly available. A broad array of programs for controlling unauthorized access and disclosure (UNAX) support IRS policy. These programs include mandatory annual UNAX training for IRS officers and employees on situations involving disclosure issues, computer security protocols permitting information access based upon assigned duties, tracking and recording of information accessed by employees, and required reports of inadvertent instances of unauthorized access or disclosure. IRM 10.5.1 defines the management structure, assigns responsibilities and uniform policies/guidance to be used by IRS employees and organizations to carry out responsibilities related to privacy, information protection and data security. It provides guidance on all aspects of protecting taxpayer and employee Personally Identifiable Information (PII). The manual section applies IRS-wide and is applicable when PII is collected, created, transmitted, used, disseminated, processed, shared, stored or disposed of to accomplish the IRS mission. It also applies to individuals and organizations having contractual arrangements with the IRS, including contractors, subcontractors, vendors and outsourced providers. IRM 10.5.4 defines the mission, objectives, and governance structure of the Incident Management Program. It provides the organizational framework for carrying out specific policies and procedures aimed at timely reaction and appropriate responses to occurrences of IRS data losses, thefts, breaches and disclosures. The provisions in this manual apply Service-wide whenever PII is collected, created, transmitted, used, processed, stored, or disposed of, in support of the IRS mission. This manual also applies to individuals and organizations having contractual arrangements with the IRS, including contractors, subcontractors, vendors, Volunteer Income Tax Assistance/Tax Counseling for the Elderly volunteers, and any other outsourced providers doing business with the IRS. Investigations of unauthorized disclosures by the office of the Treasury Inspector General for Tax Administration (TIGTA) also reinforce policy. TIGTA follows up with reports to IRS management, including recommendations for improvement. IRS management uses the IRS manager's guide to penalty determinations for appropriate disposition of each case. After consultation with its General Counsel, TIGTA refers the more egregious cases of unauthorized access or disclosure to the local U.S. Attorney for prosecution under I.R.C. § 7213 or 7213A or 18 U.S.C. § 1030. TIGTA reviews the security of IRS computers/program offices and reports its findings, with recommendations for change.	

4.3.3 Sanctions and Prior Experience	
Primary Check-list Areas	▪ Prior unauthorized disclosures ▪ Policy/process modifications to prevent future breaches
Have there been any cases in your jurisdiction where confidential information has been improperly disclosed? Have there been any cases in your jurisdiction where confidential information received by the Competent Authority from an exchange of information partner has been disclosed other than in accordance with the terms of the instrument under which it was provided? Does your tax administration or Inspector General make available to the public descriptions of any breaches, any penalties/sanctions imposed, and changes put in place to mitigate risk and prevent future breaches? If so, please provide a reference. If not, please provide a summary. (Question 3.3.3)	
Yes. The Treasury Inspector General for Tax Administration (TIGTA) maintains a website of cases of their investigations of unauthorized access to and unauthorized disclosures of confidential information that have led to criminal charges against employees. See http://www.treasury.gov/tigta/oi_highlights.shtml#28 TIGTA also conducts program evaluations of the IRS including the systems and controls in place to prevent unauthorized access to or unauthorized disclosure of confidential information. TIGTA publishes their reports of evaluations and investigations. See: http://www.treasury.gov/tigta/oie_iereports_fy14.shtml Additionally, the IRS maintains statistical data on employee (and contractor) violations and sanctions whenever unauthorized access occurs.	

4.4 Infrastructure

In order to have an effective exchange relationship between two IGA jurisdictions, each Competent Authority must feel confident that the other party has the proper infrastructure in place to fulfill its reporting obligations under the IGA (for example, requesting and receiving data from domestic Financial Institutions). To this end, the parties must have established processes for ensuring timely, accurate, and confidential data exchange, reliable communications, and capabilities to promptly resolve questions or concerns about exchange or requests to exchange. Furthermore, parties must be able to administer the compliance and enforcement provisions within the IGAs: Article 5(1) Minor and Administrative Errors and (2) Significant Non-Compliance.

4.4.1 Collection and Transmission of Information from Financial Institutions

Primary Check-list Areas	▪ Bulk information exchange processes ▪ Information protection

Does your domestic legal framework require bulk reporting of information with respect to residents' or non-residents' income or other direct tax related items? If so, what procedures does your tax administration have that describe the steps to receive/process bulk data for accounts held by Financial Institutions in your jurisdiction? How do these procedures and your information technology systems ensure confidentiality and limit the use of the data received and transmitted? (Question 3.4.1)

Yes. For example, Chapter 3 of the Internal Revenue Code, Sections 1441- 1446, requires withholding of tax by United States Withholding Agents with respect to payments to non-resident aliens and foreign corporations. Internal Revenue Regulation 1.1461-1 requires payment of the withheld tax, filing of tax returns by the withholding agent and filing of information returns by the withholding agent to report the amounts paid as well as information regarding the withholding agent and the recipient. The Form 1042-S Instructions provide the specific manner in which to complete the Form 1042-S and how to file. If the filer has 250 or more Forms 1042-S to file, then it must do so electronically. Publication 1187 provides specific guidelines for data format and submission by the withholding agent.

Similar legal and procedural requirements exist for reporting income paid to residents.

4.4.2 Prior Experience with Bulk Exchange	
Primary Check-list Areas	▪ Automatic exchange history ▪ Problem resolution ▪ Process improvements
Have you automatically exchanged bulk information on a recurring basis with treaty or TIEA partners, and have you received any feedback about the quality, usefulness and timeliness of these past exchanges? What modifications, if any, were made in response to feedback from exchange partners, and how successful were the modifications? (Question 3.4.2)	
Yes. The United States has a long history of exchanging bulk information with treaty partners. We report annually to the United States Congress Joint Committee on Taxation the volume of automatic exchange of information - JCX 8-13, Disclosure Report for Public Inspection Pursuant to Internal Revenue Code 6103(p)(3)(C) for Calendar Year 2012, for subsection k(4). The report to the Joint Committee indicates the total number of exchanges made by the IRS and the largest number are automatic although we do not separately report specific, spontaneous or automatic exchange activity. In addition, the United States Peer Review Report adopted in June 2011 describes the average number of information reports exchanged by the United States to treaty partners. We have received complaints with respect to the automatic exchange of information, and we have reported to treaty partners problems with automatic exchange of information received from treaty partners. The problems largely result from incompatible domestic reporting requirements. For example, most countries do not collect a foreign Taxpayer Identification Number which makes automatic matching of the information difficult. We are working with the OECD to develop a Schema (data collection format) that will resolve many of these problems with respect to FATCA reporting as well as broader automatic exchange of information in respect of financial institution reporting.	

4.4.3 Minor and Administrative Errors	
Primary Check-list Areas	▪ Data validation ▪ Error resolution
What is your process for validating information received from taxpayers and Financial Institutions? If your tax administration identifies data quality problems (for example, missing fields or improperly reported amounts), what steps are taken to make inquiries to the Financial Institution to resolve the data quality problems, and can penalties be assessed if these issues are not resolved within a specified period of time? (Question 3.4.3)	
The Form 1042-S Instructions specify the information to be submitted to the IRS and the method for filing returns and correcting errors that have been identified. Publication 1187 provides specific guidelines for data format and submission by the withholding agent. The IRS checks forms filed electronically and on paper, and may assess penalties for failing to timely furnish the Form 1042-S to the recipient of the payment; failing to properly complete the Form 1042-S; failing to timely file the Form 1042-S with the IRS; and failing to file Form 1042-S when required to do so. The IRS has broad enforcement powers provided for in I.R.C. § 7608 to examine any books, papers, records or other data which may be relevant to an inquiry with respect to ascertaining the correctness of any return or to create a return where none has been made. I.R.C. §7605 provides that the IRS shall fix a reasonable place and time to conduct an examination of a taxpayer.	

4.4.4 Significant Non-Compliance	
Primary Check-list Areas	▪ Resolution of significant non-compliance ▪ Policies and processes for audits and investigations ▪ Audit history
Does your jurisdiction's legal framework allow for audits of taxpayers, including the ability to demand and receive information from taxpayers and Financial Institutions? Are such audits regularly conducted, and if so, what are the characteristics of audits that have been conducted during the last [3] years? (Question 3.4.4)	
Yes. The authority specified in response to 4.4.3 applies to these questions as well. Specifically, the IRS has broad enforcement powers provided for in I.R.C. §7608 to examine any books, papers, records or other data which may be relevant to an inquiry with respect to ascertaining the correctness of any return or to create a return where none has been made. I.R.C. §7609 provides special procedures for third-party summons to obtain a third-party's testimony and records. I.R.C. §7605 provides that the IRS shall fix a reasonable place and time to conduct an examination of a taxpayer. The IRS has a robust examination program for all types and sizes of taxpayers and specifically focuses upon financial institutions through the Large Business & International Division (LB&I) Financial Services Industry. Responsibility for the Forms 1042 and 1042-S returns for payments to non-resident aliens and foreign corporations is led by LB&I International Business Compliance Foreign Payments Practice.	