Brussels, 16.3.2011

Commission report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program

17-18 February 2011

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

In accordance with its Article 13, the first review of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (the Agreement) took place six months after the entry into force of the Agreement. This review has therefore primarily focused on whether all of the elements of the Agreement have been implemented and its mechanisms have been properly put into place rather than on the effectiveness of the Agreement – time was considered too short to come to a considered judgment on that.

This report was prepared by the EU delegation of the joint review team, based on the work of the joint review team and other work independently conducted by the EU delegation. The report reflects the views of the EU delegation.

This report provides a picture of the way the Agreement has been implemented during the first six months after its entry into force. The EU review team has reached the conclusion that all of the relevant elements of the Agreement have been implemented in accordance with its provisions, including the data protection provisions. The measures which have been taken to ensure such implementation by the U.S. authorities are convincing, and in some cases go beyond what is required under the Agreement. In addition, the review team has been presented with convincing indications of the added value of the Terrorist Finance Tracking Program (TFTP) to efforts to combat terrorism and its financing. The review team met with representatives of the Treasury Department, the F.B.I., Europol, the overseers and auditors appointed by the designated provider, as well as with the overseer provisionally appointed by the European Commission.

The recommendations of the EU review team focus on the desirability of providing more publicly accessible information on the way the program functions, in as far as this is possible without endangering the effectiveness of the Program. This concerns in particular the overall volume of data provided to the U.S. authorities, and the number of financial payment messages accessed. The EU review team also suggests to further enhance the Europol verification procedure referred to in Article 4. In addition, the EU review team would welcome more verifiable statistical information on the added value of TFTP derived information to efforts to combat terrorism and its financing in order to further substantiate the added value of the program. It also recommends improving some aspects of the provision of information to the general public on the rights accorded to them under the Agreement. Finally, the EU review team provides a recommendation on the preparation of future reviews, and suggests that the implementation of the recommendations should be the subject of future review efforts.

This report consists of four Chapters. Chapter 2 provides an overview of the background to the review and its purpose and procedural aspects. Chapter 3 presents the main findings of the review and the recommendations of the review team. Finally, Chapter 4 presents the overall conclusions. The report is supplemented by Annex A which contains the report of the U.S. Department of the Treasury to the joint review team, including the answers given by the Treasury Department to the questionnaire sent on behalf of the EU members of the review team. This Annex also provides the statistical information referred to in Article 13 of the Agreement, which stipulates the elements to be covered by the review. Annex B presents the EU and U.S. representatives in the joint review team.

It is has been agreed that a follow up review will be carried out next year.

2. BACKGROUND AND PROCEDURAL ASPECTS OF THE JOINT REVIEW

Following the 11 September 2001 attacks, the U.S. Treasury Department began issuing legally binding production orders to a provider of financial messaging services whereby the U.S. Treasury would receive from that provider important volumes of U.S.-stored messaging data which would be used exclusively for the fight against terrorism and its financing. The program was called the Terrorist Finance Tracking Program (TFTP).

In mid-2006 the existence of the TFTP was made public by U.S. media. As a result of criticism within the EU, notably from data protection authorities and the European Parliament, the EU negotiated a set of undertakings (known as the TFTP Representations[1]) whereby the U.S. Treasury provided to the EU a set of EU inspired data protection conditions for the use of the EU originated data (many of which were already in place). The arrangements were to be scrutinised by an "eminent person", which turned out to be French counter-terrorism judge, Jean-Louis Bruguière. Judge Bruguière, assisted by the Commission, produced two reports, the first in December 2008 and the second in January 2010, concluding that the U.S. Treasury complies with its data protection undertakings and that the TFTP had been instrumental in preventing terrorist attacks within the EU of the magnitude of the London, Madrid and Bali attacks.

Until the end of 2009, the designated provider stored all relevant financial messages on two identical ("mirror") servers, located in Europe and the United States. On 1 January 2010 the designated provider implemented its new messaging architecture consisting of two processing zones, namely a European and a transatlantic zone.

In order to ensure the continuity of the TFTP under these new conditions, a new Agreement between the EU and the U.S. on this issue was considered necessary. After an initial version of the Agreement did not receive the consent of the European Parliament, an improved version was negotiated and agreed in the summer of 2010.

The European Parliament gave its consent to the Agreement on 8 July 2010, the Council finally approved the Agreement on 13 July 2010 and it entered into force on 1 August 2010.

The Agreement gives a central role to Europol which is responsible to receive and verify that U.S. requests for data satisfy certain conditions, including that they must be narrowly tailored so as to minimise the volume of data requested. If Europol decides that the conditions are met for any individual request, the data are transferred by the designated provider. It also contains provisions on independent overseers, including one appointed by the European Commission.

The Agreement provides for a periodical review of the implementation of the agreement. The review provisions are contained in Article 13 of the Agreement. The current report presents the EU team's findings of the first of these reviews, scheduled to take place six months after the entry into force of the Agreement.

Drawing from the content of Article 13, there are five main parameters to the review:

- the number of financial payment messages accessed;
- the number of occasions on which leads have been shared with Member States, third countries, and Europol and Eurojust;
- the implementation and effectiveness of the Agreement, including the suitability of the mechanism for the transfer of information;
- cases in which information has been used for the prevention, investigation, detection, or prosecution of terrorism or its financing;

[1] OJ C 166/18 of 20.7.2007.

– compliance with the data protection obligations specified in the Agreement.

The first joint review was carried out in Washington on 17 and 18 February 2011 with the participation of teams on behalf of both parties. In addition to three members of Commission staff, the EU team had appointed 3 experts to assist it in its tasks, namely 2 data protection experts and an expert with judicial experience, in accordance with Article 13 (3) of the Agreement. One of the two data protection experts came from a Member State where a Designated Provider is based. A full list of the members of both teams appears in Annex B.

The methodology which was developed and followed for the review exercise was the following:

– The EU team had sent out a questionnaire to the Treasury Department in advance of the review. This questionnaire contained specific questions in relation to all the aspects of the review as contained in the agreement. The Treasury provided written replies to the questionnaire.

– The joint review team was granted access to Treasury premises, including access to the site where the TFTP is operated. For security reasons, review team members were required to provide advance evidence of having a security clearance to access the TFTP facility.

– The joint review team was given a live demonstration of searches performed on the provided data, with the results shown and explained on screen by the analysts, while respecting the applicable U.S. confidentiality requirements. One member of the review team could not participate due to a lack of security clearance. However, a non-classified briefing on the searches was provided to that member of the team at a different occasion.

– The review team had the opportunity to have direct exchanges with Treasury personnel responsible for the TFTP program, the scrutineers who review the searches of the data provided under the TFTP Agreement, and the full-time auditors of the TFTP employed by the designated provider.

– The replies to the questionnaire were discussed in detail with the Treasury Department. The EU review team also had the opportunity and the time to pose further questions to Treasury officials and address all the various parameters of the Agreement.

– For the preparation of this report, the EU review team used information contained in the written replies that the Treasury Department provided to the EU questionnaire, information obtained from its discussions with Treasury personnel, as well as information contained in other publicly available Treasury documents. In addition, information obtained from the reports prepared by Judge Bruguière on the functioning of the TFTP was used, and information provided by Europol personnel, both orally and in writing. The EU team also took note of the findings of Europol's Joint Supervisory Body on its review of Europol’s involvement in the implementation of the Agreement.

Due to the sensitive nature of the TFTP, there were limitations on the provision of some documents. Some information was provided to the joint review team under the condition that it would be treated as classified up to the level of EU SECRET. Some classified information was only made available for a limited time. The review itself was conducted over a period of two days, and additional briefings and review activities occurred outside of that period. The present report should be read in the light of these considerations, as well as in the light of the fact that all members of the joint review team had to sign non-disclosure agreements exposing

them to criminal and/or civil sanctions for breaches. However, this did not hamper the work of the joint review team.

Before, during, and after the review there has been an intense exchange of views in an open and constructive spirit which covered all the questions of the joint review team. The Treasury Department provided all the information that was required by the EU review team and replied to all questions. In cases where the Treasury Department was not able to immediately provide information or documentation it provided such information at a later stage.

The EU review team would like to acknowledge the good cooperation on the part of all Treasury and other U.S. personnel, personnel of Europol and the designated provider, as well as the EU appointed temporary overseer during the review and expresses its gratitude for the way in which the questions of the joint review team have been replied to. The Commission acknowledges the professional and constructive assistance that it received from the data protection and judicial experts who participated in the EU team.

Finally, it should be noted that the procedure for the issuance of this report was agreed with the U.S. team. The EU team prepared the report. The Treasury Department was provided the opportunity to review the report for the purpose of identifying any classified or other highly sensitive information that could not be disclosed to the public.

3. THE OUTCOME OF THE JOINT REVIEW

This Chapter aims at providing the main findings resulting from the review. The Treasury Department's report to the joint review team, including the answers provided to the questionnaire of the EU members appears in Annex A. These answers also provide the statistical information referred to in Article 13.

3.1. Findings

3.1.1. Preliminary remarks

This review takes place only six months after the entry into force of the Agreement. This period is certainly long enough to review whether all of the elements of the Agreement have been implemented and its mechanisms have been properly put into place. The period of six months is however rather too short to come to a fact-based judgment of the real effectiveness of the Agreement, for reasons which are elaborated in more detail further below. The EU review team would therefore suggest that this issue is looked at in more detail in future reviews, which will take place as stipulated by Article 13 of the Agreement. For this reason, the emphasis of the review has been more on the implementation than on the effectiveness – although this latter point was also considered in detail, the EU review team came to the conclusion that whilst clear indications on the effectiveness of the Agreement have certainly been presented, more data, gathered over a longer period, would be needed to further substantiate those indications.

The EU review team also considered that it was not its task to provide a political judgement of the Agreement as such, or to suggest amendments to the Agreement – this was considered outside the scope and mandate given to the review by Article 13. The focus of the EU review team has therefore been on presenting its findings in a manner which is as objective as possible. Where recommendations are presented, these are limited to areas where the EU review team felt that their implementation would assist with further reviews, allowing a more robust future assessment of the Agreement and its effectiveness.

3.1.2. The value of TFTP in combating terrorism

There is a clear commitment of the U.S. authorities to the Agreement and its implementation. The review clarified that U.S. authorities strongly believe in the added value the TFTP brings

to the fight against terrorism and its financing. This was confirmed at all levels, from the analysts performing the searches on the database to the highest levels of policy development. At several occasions the joint review team heard that the TFTP Agreement is the most important Agreement the U.S. has in place in this area. The operational value of the program was also repeatedly confirmed by the FBI, one of the main agencies making use of the leads provided by the program.

The U.S. provided several examples of the usefulness of TFTP derived information, and the joint review team heard many testimonies to the unique value of the TFTP. Many respondents stressed the fact that although this is only one element in the overall strategy to combat terrorism and its financing, it could not be replaced by any other means. This is in particular the case since the TFTP allows not only for the identification of new links between known terrorist suspects and the people to whom they transfer funds, but also for the discovery of other identifying information of such suspects, such as bank account numbers, addresses etc. One of the main reasons for the unique value of TFTP to preventing and combating terrorism and its financing is that it allows the identification of such links also in the absence of earlier information on the bank accounts of the terrorist suspects. Banking information in general is considered very important for these sorts of investigations, since the persons concerned have a clear interest in providing accurate information to ensure that the money gets to where it is intended to go. Bank transfers are considered a reliable and accurate indicator of a link between the person sending the money and the recipient – such links must then be further investigated to establish whether they are related to terrorism.

In this context, the joint review team received confirmation that TFTP derived information is never the start of an investigation, since a terrorism nexus needs to be proven before the database may be searched, but also never the end of an investigation, since the leads identified always need further investigation by the services concerned.

The number of leads provided since the start of the program and since the entry into force of the Agreement indicates a continued benefit for preventing and combating terrorism and its financing across the world, with a particular focus on the U.S. and the EU. The added value of the TFTP was also confirmed by Europol, which received a number of leads from the U.S. authorities during the first six months the Agreement has been in force.

The joint review team was also informed that in many cases the value of the TFTP is not recognised as such even by the recipients of TFTP derived information, either in the U.S. or abroad. This is due to the fact that the general practice is to provide such information to the responsible agencies in a way which does not disclose the methods or procedures for capturing it – it is usually provided to third parties without indications where the information came from. One concrete example was discussed by the review team where a prosecutor in one of the Member States had questioned the added value of TFTP derived information, simply because he was not aware that the information provided and used had been derived from the program.

In addition, there is the general difficulty of assigning a concrete value to information derived from the TFTP since it is normally only one piece of the puzzle of an investigation. In many cases, it is therefore difficult to assess whether this one piece of the puzzle was decisive for the overall investigation, without looking into each and every detail of an investigation. Leaving aside the need for confidentiality of ongoing investigations, such detailed assessment was clearly outside of the scope of the current review.

Nevertheless, the joint review team was presented with indirect indications of the value of TFTP derived information to counter-terrorism investigations: e.g. the number of requests for such information from the FBI has consistently gone up over the years that the program has been in place, demonstrating that this information was perceived as offering added value to

ongoing terrorism investigations. In addition, the joint review team was presented with (classified) information on a number of high profile terrorism cases where TFTP derived information had been used. Data was also provided on the number of leads shared with EU Member States, Europol and third countries.

Taking note of these general indications that the TFTP provides added value both to U.S. and EU authorities in preventing and combating terrorism and its financing, the EU review team is of the opinion that efforts should be made to further substantiate the added value of the program, in particular through more systematic monitoring of the results obtained through the program and the Agreement by both U.S. and EU authorities. Treasury should seek feedback from the agencies which receive TFTP derived information on a systematic basis in order to verify the added value of the information. Europol could play a role in coordinating an effort to collect such feedback on the EU side. Such feedback would however only be expected to return appropriate results after the Agreement has been in force for a longer period of time, since the real added value of information received can only be properly evaluated once the investigation in which it has been used has been closed. This is therefore an appropriate subject for further review. In particular, statistical information supporting the effectiveness of the TFTP would be valuable. So far, there have been no indications that the safeguards included in the Agreement have reduced the efficiency and proper functioning of the TFTP.

The EU review team recommends that more feedback is collected and analysed by EU and U.S. authorities in order to provide more verifiable insights into the actual added value of the TFTP through eliciting feed-back from the users of TFTP derived information, whilst respecting the need for confidentiality of the methods and procedures used.

3.1.3. Statistical information and confidentiality issues

Assessing the added value of the TFTP and communicating clearly and openly about the implementation of the program and the Agreement can only be done in so far as this does not jeopardise the ongoing value of the program. The U.S. authorities have on many occasions expressed their concern to ensure that no details of the program would become public which could harm the effectiveness of the program. This concern was also demonstrated by the procedures on security clearances and the non-disclosure agreements which the members of the joint review team were asked to sign. The EU review team believes that this is a fully justified concern, given the importance of the program to preventing and combating terrorism and its financing.

This need for confidentiality necessarily limits the possibilities to communicate some details on the implementation of the TFTP and the Agreement, whilst there is a clear interest in such details from interested parties. Two examples of the tension this can create were discussed in particular by the joint review team – the overall volume of financial payment messages provided under the Agreement to U.S. authorities, and the number of searches which were performed on this data.

As to the first point (the overall volume of financial payment messages provided): even though this is not formally included in the scope of the review under Article 13, there is a clear interest from many sides to be informed on this point in order to fully understand the scope of the program, its possible implications on civil liberties, and thus its proportionality. The discussion on this point demonstrated the difficulties referred to above. Whilst at first sight it would appear harmless to make an overall figure public, the U.S. authorities argued that providing this information could in fact be detrimental to the effectiveness of the program. Their reasoning centred around the fact that they want to ensure the confidentiality of the message types and the geographical regions covered by their requests under the Agreement. If these were to become known, terrorists could undermine the effectiveness of

the program by avoiding the usage of such message types in these regions. The arguments were made that providing indications of the overall volume of data provided would in fact provide indications as to the message types and geographical regions sought (in combination with other publicly available information) and that this was outside the scope of the review under Article 13.

The second point (the number of financial payment messages accessed) is covered explicitly by the scope of the review, as indicated in Article 13. In this case, the joint review team was provided with the overall number of searches made of the provided data since the entry into force of the Agreement. This number is included in Annex A to this report. However, the EU review team discussed that without an idea of the overall volume of data provided, the total number of searches performed does not provide a reliable indicator of the proportionality of the amount of searches. What can be clearly mentioned, however, is that the overall number of searches indicates that only a small proportion of the data provided is in fact accessed as a result of the searches performed. This demonstrates that the safeguards put in place to ensure that all searches of the database can only be performed if there is a clear terrorism nexus do work in practice.

Furthermore, the initial phase of implementation of the Agreement has met with a considerable degree of interest amongst stakeholders. For instance, the European Commission has replied to 16 questions posed by Members of European Parliament[2], which were subsequently circulated to Member States and shared with the Treasury Department. These replies, together with the Commission's oral explanations (e.g. in the LIBE Committee of the European Parliament or in the Management Board of Europol) should contribute to a better understanding of the Agreement.

To conclude on this point – whilst the EU review team fully subscribes to the need to ensure that no information becomes part of the public domain which would harm the effectiveness of the TFTP and the Agreement[3], it also notes that without concrete information on the overall volume of data exchanged under the Agreement, a statistical assessment of the effectiveness and implementation of the Agreement will remain a significant challenge. The EU review team therefore recommends that future reviews should keep a clear focus on transparency issues.

The EU review team recommends that more statistical information on the overall volumes of data provided under the Agreement and the data accessed is provided in the course of future reviews – such information should preferably be public information, where this is possible without endangering the effectiveness of the TFTP. Options should be explored to provide more regular information on the effectiveness and implementation of the TFTP, e.g. by way of six-monthly updates, which could also include questions and answers.

3.1.4. Are requests for data "as narrowly tailored as possible" - the role of Europol

The discussion on overall volumes of information requested, provided and accessed is linked to the interpretation of the words "as narrowly tailored as possible" as used in both articles 4 (2) (with respect to the data requested of the designated provider) and Article 5 (6) (with respect to the searches made of the data). The EU review team recognises that although the wording of these phrases is similar, there is a clear difference in the practical effects of the application of this terminology. The reason for this is simple – whilst the Agreement requires that every effort is made to ensure that the *categories of data* which are requested from the

[2] E-5139/2010, E-5141/2010, E-5142/2010, E-5144/2010, E-6094/2010, E-6838/2010, E-6873/2010, E-7516/2010, E-7517/2010, E-7518/2010, E-8060/2010, E-8327/2010, E-8410/2010, E-9872/2010, E-10410/2010, E-11200/2010.

[3] In this context the leaking of the Technical modalities agreed under Article 4 is considered unfortunate.

designated provider are as narrowly tailored as possible, in effect the TFTP – and by extension the TFTP Agreement - can not work effectively without the provision of significant amounts of data, since it is impossible to predict in advance which part of that data will be relevant to a terrorism investigation.

The Agreement requires Europol to verify that the request for such data identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the prevention, investigation, detection or prosecution of terrorism and its financing. In addition, Europol should verify that the request is "tailored as narrowly as possible in order to minimise the amount of data requested, taking due account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities, geographic, threat and vulnerability analyses and not seek any data related to the Single Euro Payments Area."

Europol informed the EU review team that the requests which it had received for verification would typically include categories of financial messages sought, the relevant time-period and the geographic scope, and that the request would be accompanied by supplementary documents. The information provided by the U.S. also includes elements justifying why certain categories of messages are requested and why a specific geographical scope was chosen. The requests are classified by Europol at the level of EU Secret. In addition to these supplementary documents, Europol bases its judgment on the professional background of the Europol officials involved, information from its own counter-terrorism unit, as well as on the confidential oral briefings these Europol officials receive on a quarterly basis from U.S. authorities. If Europol is not satisfied with the level of information provided, it seeks additional information from the U.S. authorities, which has happened already on a number of occasions. Europol has also confirmed that no request of the U.S. was aimed at obtaining SEPA-related data, and the designated provider has confirmed that no SEPA-related data have been provided to the U.S.

The joint review team was provided with a redacted version of the latest request that the U.S. authorities had presented to Europol. On this basis, it discussed the issue of variation in the requests, and the way U.S. authorities aim to ensure that the requests are as narrowly tailored as possible. One of the elements considered is the fact that the terrorism threat situation, and the relevant geographical zones, have not changed significantly over the period of six months covered by the review, even though there had been a few incidents, such as the threat from parcel bombs sent to a variety of destinations in the EU and elsewhere. The joint review team was informed that the scope of the requests put to the designated provider has been significantly reduced since the start of the program, based on a thorough annual analysis which indicated which of the message categories and geographical regions covered provide the most added value for terrorism investigations.

The joint review team was in fact presented with (classified) information which demonstrated that the scope of the requests made of the designated provider has indeed been more narrowly tailored since the entry into force of the Agreement as a consequence of the review of the usefulness of such data to counter-terrorism purposes performed in 2010.

The EU review team was also informed of the conclusions and recommendations of Europol's Joint Supervisory Body (JSB), which has examined the role of Europol in this respect. The JSB is of the view that U.S. authorities should provide as much relevant information as possible to Europol in writing, since the information provided during oral briefings can not be verified independently after the fact. The EU review team is of the opinion that there seems to be scope to provide more detailed and targeted justifications for the requests to the designated provider in writing in order to enable Europol to perform its functions even more effectively.

In conclusion, the EU review team is satisfied that the procedures required under the Agreement have been put in place to ensure that, in principle, the requests for information are tailored as narrowly as possible, and are also in line with the other requirements of the Agreement. Europol clearly takes its role under the Agreement very seriously, and has put in place all the necessary elements to fulfil its role in accordance with the Agreement and its implementing technical modalities. The U.S. authorities from their side also have an interest to ensure that the request only relates to data which are actually relevant for counter-terrorism purposes, since only those data provide real added value, and have taken appropriate steps to amend the requests accordingly. They have also demonstrated a clear commitment to support Europol in its new role under the Agreement, and the cooperation between Europol and the U.S. authorities in this respect has been seen as positive by both parties. The EU review team is also content that it was presented with evidence demonstrating that the interaction between the two parties and the annual review have led to a reduction in the scope of the information requested during the first six months of the Agreement. It would however urge U.S. authorities to provide as much information as possible to Europol in writing, even where such information is classified, in order to allow further verification of the way in which Europol fulfils its role under the Agreement, including by way of future reviews.

The EU review team recommends that as much (classified) information as possible substantiating the requests is provided to Europol in a written format in order to support it in its tasks under Article 4 and to allow for more effective independent review.

3.1.5. Are searches of the provided data "narrowly tailored" – safeguards and oversight

The Agreement (Article 5) provides that safeguards are put in place to ensure that the provided data is only accessed in cases where there is a clear nexus to terrorism, and where *the search of the data* is narrowly tailored. The U.S. Treasury is responsible for ensuring that provided data are only processed in accordance with the Agreement. These safeguards are intended to ensure that only a very small proportion of the data provided is ever accessed by such searches, since the number of persons investigated for involvement with terrorism or its financing is limited. As mentioned above, this also means that by far the largest number of data will never be accessed, and the fact that such data has been provided to U.S. authorities will thus not produce any noticeable effect on the persons whose data is not accessed. Leaving aside the issue of the overall number of searches performed on the data, as discussed above under 3.1.3, the joint review team focused its efforts on verifying that the safeguards described in Article 5 have indeed been put into place and function as intended. In addition, the joint review team focused specifically on the oversight described in Article 12 of the Agreement, and how this impacts the effectiveness of these safeguards.

Technical provisions have been put in place which ensure that no search can take place without the entry of information on the terrorism nexus of the search. Also, it was confirmed that all these searches are logged. The analysts operating the searches also confirmed that the searches are tailored as narrowly as possible, and this meets both operational and data protection considerations. The operational effectiveness of the system would suffer from searches which are not narrowly tailored, since these would return too many results and thus too much irrelevant data. Analysts are continuously trained on how to ensure that searches are narrowly tailored and how the terrorism nexus must be demonstrated before searches are allowed. Those who do not respect the applicable safeguards are either required to undergo further training, or their access to the database is revoked.

In addition, the respect of these safeguards is ensured through the work of independent overseers, as referred to in Article 12 of the Agreement. The joint review team had the opportunity to speak to the most senior of these overseers, which are normally appointed by the designated provider and in its employment, as well as to the person who had been

appointed to provisionally act as EU appointed independent overseer.[4] The joint review team was informed that these overseers see and verify all of the searches performed on the provided data. In accordance with the provisions of the Agreement, they have the possibility to review in real time and retro-actively all searches made of the provided data, to request additional information to justify the terrorism nexus of these searches, and the authority to block any or all searches that appear to be in breach of the safeguards laid down in Article 5. The overseers confirmed that they had made full use of these powers: they request additional information on an on-going basis, and all overseers, including the EU appointed one, had blocked searches to request additional information. The joint review team discussed with the overseers whether real-time or retroactive review was more effective. In their view the retroactive review was more suitable for a thorough examination of the searches, since it afforded a longer time period to reach a decision whether or not to block the dissemination of the results of the search. Normally, a retroactive review of the searches will take place within 24 hours of the execution of the search.

In those cases where the search had been questioned or blocked by the overseers, additional information was provided by the U.S. authorities. Some of these cases are further discussed between the overseers and Treasury personnel in so-called reconciliation meetings. Other than in exceptional circumstances, no search results had been disseminated until an overseer had had an opportunity to review the search – a safeguard which goes beyond those specified in the Agreement. The continuous education of the analysts and their awareness of the safeguards imposed has ensured that whilst all searches had been reviewed, the request for additional information or discussions in reconciliation meetings have been limited to a very small percentage of cases.

The overseers also confirmed that the cooperation between the EU designated provisional overseer and the overseers appointed by the designated provider had been very good, and that close cooperation and the sharing of experiences between them had ensured that the EU overseer had quickly been able to perform his duties in line with the requirements.

In conclusion, the EU review team is of the opinion that the system of independent oversight over the implementation of the safeguards incorporated in the Agreement is a unique and powerful tool to ensure that these safeguards are respected. The EU review team is unaware of any other law enforcement or intelligence gathering or analysis program which functions under comparable continuous independent oversight. In this context, the EU review team notes that it considers the power to block the dissemination of the results of searches more important than the power to block the search as such, since it is only the dissemination of the results which may produce concrete consequences for the persons concerned.

3.1.6. Data security and integrity – independent audit

The EU review team is convinced that the measures taken to ensure data security and integrity are adequate. During the review visit, it became clear that the utmost care has been taken by the U.S. authorities to ensure that the data is held in a secure physical environment, that there can be no unauthorised access to the data, that the data are not interconnected with any other database, that the provided data shall not be subject to any manipulation, alteration or addition, and that no copies of provided data should be made, other than for recovery back-up purposes. This conviction is based on the measures observed during the visit to the location where the data are queried, the answers provided both in writing and orally in the course of the review, and on the conversation with the independent auditors, who monitor the implementation of these safeguards on a daily basis. These auditors, who are engaged by the designated provider to verify the implementation of the safeguards agreed between the designated provider and the U.S. authorities, provide quarterly reports on their activities to the

[4] In the meantime, a "permanent" overseer has been appointed.

designated provider. For a future review, access to these audit reports, if made available by the designated provider, could provide further certainty on this point. The EU review team noted that this independent audit goes beyond the safeguards stipulated explicitly in the Agreement, and provides welcome assurance.

3.1.7. Data protection provisions

The most relevant Articles on data protection are Articles 6, 14, 15 and 16, as well as Article 18. The Treasury explained that so far little use has been made by individuals of the possibilities to exercise their rights under the Agreement (see Annex A).

3.1.7.1. Retention and deletion

As to the retention and deletion of data, not much can be said at this stage. According to the provisions of article 6, the first deletion of data should take place not later than 20 July 2012. All non-extracted TFTP data the U.S. has received from the EU prior to 20 July 2007 should at that date be deleted from all systems. The Treasury has confirmed the plans to carry out this initial deletion of data by July 2012, and has confirmed that it has already deleted portions of the data over time. This means that up to the moment of the review, the U.S. had TFTP data stemming from the period late 2001 to early 2011 available.

3.1.7.2. Transparency – providing information to data subjects

As required by article 14 of the Agreement, the Treasury has set up a specific website with information on the Terrorist Finance Tracking Program, to be found at http://www.treasury.gov/tftp. The website contains a general description of the TFTP, written to be understood by the general public, as well as a document containing frequently asked questions and their answers. Furthermore, documents can be found on the website explaining to individuals how they can exercise their rights under the agreement.

Apart from their website, the Treasury also has an e-mail service available, as well as a telephone hotline. Both were already in place for general information to the public, but have explicitly been extended in order to deal with additional information requests on the TFTP Agreement. The employees that man the helpdesk were given additional training on the implications of the Agreement and the working of both the TFTP and the redress procedures.

The telephone hotline, a free phone number accessible within the U.S. and a Washington phone number accessible from abroad, has a special option in the dial menu which leads to more information on the TFTP. The automatic message the individual receives refers to the Treasury website and has the possibility to leave a voicemail message. Personnel of the Treasury helpdesk will call back the individual if possible within 24 hours. So far, several hundred voicemail messages were recorded, none of which contained specific questions on the TFTP. No phone calls were received from individuals requesting to exercise their rights under the Agreement.

The specific e-mail account set up by the Treasury to answer questions on TFTP (tftp@treasury.gov) has so far only been used once, by an EU citizen who wanted to know more on the ways he could find out if his information was indeed stored in the TFTP database. The person in question was given an extensive reply, informing him both on the possibility to request access through his national Data Protection Authority (NDPA) and under the U.S. Freedom of Information Act.

3.1.7.3. Right of access

Upon the entry into force of the Agreement, the Treasury has set up the procedures for individuals to seek access to their personal data under the TFTP Agreement. This procedure, which is described in detail on the Treasury website, has to comply with U.S. national law as well as the Agreement. This means the procedure is set up as follows.

The individual should send the request, which needs to be as specific as possible, to his National Data Protection Authority (NDPA). The request should be done in writing and is to signed by the person making the request. Furthermore, he/she has to include a copy of proof of ID (passport, driver's licence, etc.), as well as a statement authorising the Treasury to disclose personal data to the NPDA. Subsequently, the NPDA is to forward the original request, including the documents mentioned before, to the Treasury's Office of Privacy and Civil Liberties (OPCL). The OPCL staff review the request and contact the Program Office responsible for the TFTP. That Office conducts the review pursuant to the request and feeds back information to the OPCL staff. If there is indeed a responsive record, this record is reviewed to decide whether the information can be released to the individual. That decision is taken by the TFTP Program Office and is reviewed by the OPCL. Finally, the OPCL prepares and issues the response to the request to the NDPA, which should subsequently inform the individual.

The joint review team discussed this procedure in detail, and questioned the need for an individual to disclose additional personal information to the U.S. authorities in order to exercise their data protection rights. These discussions clarified that the proof of ID and the consent statement are required under U.S. law. Both the Director of OPCL and the Deputy Assistant Secretary for Privacy, Transparency & Records of the Treasury, the department overseeing the OPCL, recognised the issue but explained they were required by law to verify the identity of the individual making the request. They ensured the joint review team, however, that since they deal with privacy issues continuously, their department is very aware of the need for protection of personal identifiable information. The OPCL will treat the request and additional documents with care and will not forward the additional documents to the TFTP Program Office. They remain with the privacy officer dealing with the access request.

So far, no specific completed requests from individuals wishing to exercise their rights under the Agreement have been received, neither directly nor through an NDPA.

As described above, upon request from an individual, it is the TFTP Program Office that will conduct a review of the records to see whether there is a responsive record. A responsive record means, that the TFTP database contains information about the individual in question which was indeed accessed by the analysts in the course of an investigation with a nexus to terrorism. As indicated above, under the Agreement, the Treasury is only allowed to access the database if that nexus is clearly established. That also means, that there is no possibility for the Treasury to search the database for information of individuals which was not accessed before. In those cases, there would be no demonstrable nexus to terrorism which would allow for access to information stored in the black box the TFTP database is. Such a search would thus violate the purpose limitation provisions of the Agreement. Although this may seem unsatisfactory to the individual - it would mean there is only a very limited part of the database for which the right of access applies - the EU review team is of the opinion that this procedure is a correct implementation of the Agreement.

3.1.7.4. Right to rectification, erasure or blocking

The procedures to exercise the rights to rectification, erasure or blocking are similar to the procedure described above for the right of access, although of course the content of the request would need to be different. Also, the individual would need to specify which right is being sought.

The data provided under the Agreement can not be changed or altered to ensure the integrity of the database, as stipulated by Article 5 (4)(d). The Treasury explained that, as a consequence, it had to devise a different way to deal with requests for rectification, erasure or blocking of information. This means that if a request is indeed justified, the data will either be

blocked, or flagged to indicate that such data can no longer be relied upon. The Treasury also confirmed that in those cases where erroneous information had already been supplied, the recipients would be informed about the incorrect nature of the information provided.

The Treasury furthermore explained, that they would refer individuals with a request for rectification or erasure of information from a bank transfer to their own bank. That bank is the only institution that could in fact make amendments to the original record, by sending out a new financial transaction message with the new information. To the extent that the original record was transmitted to the Treasury under the TFTP, this new record would likely be included in a next transfer of data to the Treasury and thus be included in the TFTP database.

As explained before, the only changes that can be made to the TFTP database as such are the consequence of an updated financial transaction message the original bank institution may send. Such messages would normally be included in a future request for transaction data to be transferred from the designated provider to the Treasury. It is however unclear, also because there has not been any example so far, in what way the Treasury would discover such an updated financial transaction message. In most instances, that would not be a problem, except for when the original data which is then being updated was accessed by an analyst. The EU review team concludes there is a minor risk that the rectified information would not be seen by an analyst and that subsequently the old/wrong information from the original record is used and may be forwarded to other agencies or third parties.

The EU review team recommends that more information on the factual possibilities and impossibilities for rectification, erasure and blocking of information should be posted on the website of the Treasury, for instance in an updated version of the document with frequently asked questions.

3.1.7.5. Redress

Under article 18 of the Agreement, individuals have several possibilities for redress, both under European law and under U.S. law. During the review, only the U.S. redress mechanism was discussed.

The first possibility in the redress procedure is the appeal against administrative actions. This appeal may follow if a request of access, rectification, erasure or blocking of data has ended unsatisfactory for the individual concerned. He/she may then go back to the NDPA to submit a request to review the original decision from the OPCL and the TFTP Program Office. This new request is to be sent to the Deputy Assistant Secretary (DAS) for Privacy, Transparency & Records, who is the main official responsible for the OPCL. This request also has to be accompanied by a proof of ID and a consent for the disclosure of personal data to the NDPA. The DAS will personally review the request, based on the full documentation supplied by the TFTP Program Office. The decision of the DAS is the final agency decision and will be reported back to the NDPA. Should the individual still not be content, he/she may appeal against the final agency decision under the U.S. Administrative Procedure Act.

Another possibility for redress is to start a procedure under the U.S. Freedom of Information Act (FOIA). Such a request should be addressed to the Treasury Disclosure Services Office. Ordinarily, FOIA requests should always be granted, except when one or several of the specified exemptions apply. These include matters that are properly classified in the interest of national defence or foreign policy and certain information compiled for law enforcement purposes. Decisions on an FOIA request may be appealed against in a U.S. federal court, whatever the nationality or normal place of residence of the appellant. The appeal can take place in several instances, up to the Supreme Court.

Finally, persons who believe their property has been blocked by the Office of Foreign Assets Control (OFAC) in reliance on inaccurate personal data from the TFTP can request that this

blocking is reconsidered. Should a person suffer from damages or loss in connection with the use of his/her data under the TFTP, then he/she would be allowed to seek compensatory damages and injunctive or equitable relief under the Computer Fraud and Abuse Act.

3.1.8. Preparation of an EU system equivalent to the TFTP

Article 11 of the Agreement stipulates that during the course of the Agreement, the European Commission will carry out a study into the possible introduction of an equivalent EU system allowing for a more targeted transfer of data, and that if, following this study, the European Union decides to establish an EU system, the U.S. shall cooperate and provide assistance to contribute to the effective establishment of such a system. Following the entry into force of the Agreement on 1 August 2010, the Commission had started with preparatory actions to come to the establishment of an EU equivalent system. These actions have included the start of the study referred to in Article 11, and have also included the organisation of a number of expert meetings to consult with representatives of EU Member States and other parties concerned, such as data protection authorities.

The EU review team recognises the assistance provided to these activities by the U.S. Treasury Department. At the second of the expert meetings, organised on 21 January 2011, a strong delegation of experts from the Treasury participated, and presented a comprehensive overview of the way the TFTP functions in the context of the overall U.S. counter-terrorism efforts and the implementation of the Agreement. In addition, the U.S. delegation answered openly and transparently to all questions which were raised by the representatives of the Member States and the data protection authorities. Based on its experiences, the U.S. delegation also provided a number of concrete indications of issues which should be considered by the EU in the establishment of an equivalent system.

Also, representatives of the U.S. Treasury have made themselves available for further contacts during the preparation of the report referred to above. The EU review team recognises these efforts as a welcome sign of the willingness of the U.S. authorities to assist the EU in its considerations of the creation of an EU system equivalent to the TFTP, and thus of the implementation of Article 11 of the Agreement.

3.1.9. Security clearance

As noted above, participation in the review by EU team members was conditional on having demonstrated proof of national security clearance up to the level of EU Secret. Since one member of the EU delegation did not have such clearance, that member could not participate in part of the visit and some of the discussions. Also, that member was not allowed to see all relevant documentation, although a non-classified briefing was provided to that member of the team on a different occasion. Although the requirement of an appropriate security clearance for participation in the review is certainly reasonable, the EU review team would suggest that in future reviews, this requirement would be communicated further in advance of the actual review, giving an opportunity for all team members to ensure that they have the necessary clearance. It is also suggested that the parts of the review agenda which require such security clearance would be indicated well in advance.

The EU review team recommends that in the preparation of future reviews more timely information is provided on the security clearances required for parts of the review.

3.2. Recommendations for improvement

Based on the findings presented above, the EU review team presents the following recommendations:

- it is recommended that more feedback is collected and analysed by EU and U.S. authorities in order to provide more verifiable insights into the actual added value of the TFTP through eliciting feed-back from the users of TFTP derived information, whilst respecting the need for confidentiality of the methods and procedures used (3.1.2);
- it is recommended that more statistical information on the overall volumes of data provided under the Agreement and the data accessed is provided in the course of future reviews – such information should preferably be public information, where this is possible without endangering the effectiveness of the TFTP. Options should also be explored to provide more regular information on the effectiveness and implementation of the TFTP, e.g. by way of six-monthly updates, which could include questions and answers. (3.1.3);
- it is recommended that as much (classified) information as possible substantiating the requests is provided to Europol in a written format in order to support it in its tasks under Article 4 and to allow for more effective independent review (3.1.4);
- it is recommended that more information on the factual possibilities and impossibilities for rectification, erasure and blocking of information is posted on the website of the Treasury, for instance in an updated version of the document with frequently asked questions (3.1.7.4);
- it is recommended that in the preparation of future reviews more timely information is provided on the security clearances required for parts of the review (3.1.9).

Finally, the EU review team would recommend that the implementation of these recommendations will form part of future reviews.

4. CONCLUSIONS

Keeping the limitations of the current review in mind, the EU review team is of the opinion that the review mechanism as such is a valuable tool for the assessment of the level of implementation of the Treasury Department of the agreement, and its compliance with the safeguards included therein. The EU review team is also of the opinion that this Agreement needs to be assessed on the basis of all its elements, since it is only through a clear look at the combined effects of these elements that a provisional judgment can be formed. This overall view of all relevant elements presents an image of a very sensitive program, which has been very well protected, and is scrupulously managed in accordance with a set of effective safeguards, some of which go beyond what is required under the Agreement. Respect for these safeguards is ensured by independent oversight and audit practices which go beyond those put in place for comparable government programmes, and which inspire significant confidence that the safeguards are in fact respected. In addition, the data protection provisions and systems which have been put in place meet the requirements of the Agreement. The review team has been provided with convincing indications of the added value of the TFTP to the fight against terrorism and its financing.

Perhaps unsurprisingly, all of the EU review team's recommendations for improvement are therefore not so much addressed towards the TFTP and the implementation of the Agreement as such, but rather at improving the level of information which can be shared with future review teams and the public at large. The EU review team is convinced that more

transparency on the added value of the program to the fight against terrorism, on the overall volumes of data concerned and on other relevant aspects would go a long way in convincing a wider audience of the real benefits of the TFTP and the Agreement, as well as raise the level of trust towards the program, and that such transparency should be sought wherever possible without endangering the effectiveness of the program as such.

It is has been agreed that a follow up review will be carried out next year.

ANNEX A
TREASURY REPORT TO THE JOINT REVIEW TEAM

Pursuant to the U.S.-EU

Terrorist Finance Tracking Program Agreement

February 2011

After approval from the European Commission, Council, and Parliament, and signature by representatives of the United States and the European Union, the *Agreement Between the United States of America and the European Union on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program* ("the Agreement") entered into force on August 1, 2010. Pursuant to Article 13 of the Agreement, the Parties shall conduct a regular joint review of "the safeguards, controls, and reciprocity provisions" of the Agreement.

In preparation for the first review, scheduled for February 17-18, 2011, in Washington, D.C., the U.S. Department of the Treasury ("Treasury Department") hereby provides information on the implementation of the Agreement for the six-month period from its entry into force through January 31, 2011, and responds to a questionnaire submitted by the European Commission ("Commission") on behalf of the European Union ("EU") joint review delegation.

I. Background

As part of the Terrorist Finance Tracking Program ("TFTP"), the Treasury Department issues administrative production orders ("Requests") to the Society for Worldwide Interbank Financial Telecommunication ("the Designated Provider"), a provider of international financial payment messaging services, for narrow sets of financial messaging data transmitted between financial institutions that are relevant to counter-terrorism investigations. Requests are narrowly tailored based on past analyses of relevant message types, geography, and perceived terrorism threats. The subsets of data transferred to the Treasury Department pursuant to the Requests are subject to strict security measures and cannot be searched except where various elaborate safeguards are satisfied.

Pursuant to the Agreement, the Treasury Department provides a copy of Requests for data stored in the EU, along with any supplemental documents, to Europol to verify whether the Requests (a) clearly identify the data requested; (b) clearly substantiate the necessity of the data; (c) are narrowly tailored; and (d) do not seek any data relating to the Single Euro Payments Area ("SEPA"). Once that verification has occurred, Europol is to notify the Designated Provider, and the Designated Provider will transmit the data to the Treasury Department.

II. Implementation of the Agreement

The Treasury Department's implementation of the Agreement began immediately after its entry into force. On August 2, 2010, the first business day after the entry into force, the Treasury Department implemented the terms of Article 14 of the Agreement – Providing Information to the Data Subjects – and posted on its public website detailed information concerning the TFTP and its purposes, including (1) contact information for persons with

questions and (2) information regarding administrative and judicial redress procedures available for all persons, regardless of nationality or place of residence.[5]

On August 4, 2010, the Treasury Department provided Europol with its first Request, along with supplemental documents, pursuant to the Agreement. On August 3-4, 2010, Treasury Department officials also conducted a series of briefings, including a classified briefing related to current counter-terrorism threats, for Europol officials in Washington to provide additional detail regarding the necessity of the data and the narrow tailoring of the Request. Europol verified the Treasury Department Request on August 10, 2010, and thereafter notified the Designated Provider.

As the Europol process was ongoing, the European Commission requested that the Treasury Department approve an interim EU overseer, pending a thorough search for a permanent overseer, to be effective on or before the date of any searches of data provided pursuant to the Agreement. On August 26, 2010, the day the initial EU-provided data were loaded into the TFTP and available for search, the interim EU overseer began his duties in Washington; the interim EU overseer has since reviewed searches from August 1, 2010, onward, before the Treasury Department received any EU-provided data.

On January 11, 2011, Commissioner Cecilia Malmström notified the Treasury Department of her selection of a candidate for the permanent EU overseer. The Treasury Department subsequently agreed to the appointment, pursuant to the terms of the Agreement.

Although these have been some of the more notable aspects of the implementation of the Agreement, the Treasury Department has worked to ensure robust completion of all objectives and responsibilities set forth in the Agreement. In addition, over the past six months, the Treasury Department has received and briefed, on a regular basis, various delegations from EU institutions and EU Member State Governments, Parliaments, and data protection authorities. Treasury Department officials also have traveled to Brussels and The Hague in furtherance of the implementation of the Agreement, including by providing a presentation in Brussels in January 2011 to assist the EU as it studies whether to institute an equivalent EU system to the TFTP.

Additional details regarding the Treasury Department's implementation of the Agreement are provided below, in response to a questionnaire submitted to the Treasury Department on behalf of the EU joint review delegation.

III. Treasury Department Response to EU Questionnaire

The questionnaire submitted by the EU joint review delegation is reproduced in bold, below. The Treasury Department's responses follow each question.

I. Statistical information

1. How many financial payment messages were accessed since the entry into force of the Agreement?

In the six months between August 1, 2010, and January 31, 2011, TFTP analysts conducted 27,006 searches of the TFTP. This number includes searches involving data stored in and

[5] The Treasury Department subsequently received informal comments on its redress procedures from EU data protection authorities and the European Commission, and it revised its procedures to accommodate many of those comments, posting a new version on August 31, 2010. The TFTP materials are available at www.treasury.gov/tftp.

obtained from the United States, as well as data stored in and obtained from the EU pursuant to the Agreement. This number includes searches of financial payment messages from financial institutions around the world, most of which involve neither the EU nor its residents.

A single investigation may require numerous TFTP searches. Each TFTP search may return multiple results or no results at all. Searches that yield multiple results may allow analysts to determine from the search results whether individual messages should be viewed, and thereby accessed, or whether they need not be accessed. In addition, the overwhelming majority of messages that are accessed will never be disseminated or even printed; most will be viewed for a few seconds to determine value and thereafter closed, with no further action or dissemination.

2. In how many occasions was information derived from accessing these payment messages provided to competent EU authorities, including Europol and Eurojust?

In the six months from August 1, 2010, to January 31, 2011, U.S. investigators supplied 84 reports resulting from TFTP data to competent authorities of EU Member States and EU authorities, such as Europol. Such reports generally summarize the results of an investigation of a subject, which will typically encompass multiple TFTP searches, each potentially retrieving numerous messages. More than 1,700 such reports have been provided to the EU in the nearly 10 years since the program began.

3. In how many occasions was information derived from accessing these payment messages provided to third countries?

Between August 1, 2010, and January 31, 2011, U.S. investigators supplied 31 reports resulting from TFTP data to the competent authorities of third countries. As described in response to Question 2, above, such reports generally summarize the results of an investigation of a subject, which will typically encompass multiple TFTP searches, each potentially retrieving numerous messages. More than 2,500 such reports have been provided to competent authorities throughout the world since the program began, the overwhelming majority of which (1,700) have been provided to the EU.

4. In how many cases was information provided spontaneously, in accordance with Article 9 of the Agreement?

Seventy of the 84 reports provided during the relevant six-month period to EU Member States and EU authorities, such as Europol, involved the spontaneous provision of information.

5. How many EU requests for TFTP searches in agreement with Article 10 of the Agreement have been received? In how many cases did these requests lead to the transmission of information?

The Treasury Department received 15 requests pursuant to Article 10 in the period from August 1, 2010, to January 31, 2011. It provided leads to the EU in response to all 15 requests – a 100 percent return rate. In at least one case, the Treasury Department supplied additional spontaneous information beyond that requested by the EU in its Article 10 request.

II. Implementation and effectiveness of the Agreement

6. During the period of the review, have there been any particular concerns with respect to the suitability of the mechanism for the transfer of the information?

No.

7. What has been the frequency of Requests to Europol and the Designated Provider under Article 4 of the Agreement?

The Treasury Department has submitted its Article 4 Requests on a monthly basis since the adoption of the Agreement.

8. What procedures have been put in place to ensure that the Requests are tailored as narrowly as possible as required under Article 4 (2) (c)?

The Treasury Department performs a continuous review of the data received and the utility and necessity of the data for counter-terrorism purposes. A large-scale audit and analysis of the extracted data – spanning several months and requiring hundreds of employee hours – is conducted every year, analyzing on a quantitative and qualitative basis the types of data most responsive or relevant to counter-terrorism investigators, and the geographic regions where the terrorist threat is particularly high or most relevant or susceptible to relevant terrorist activity.

As a result of this comprehensive analysis, the Treasury Department historically has refined and reduced the scope of the data requested. Because the Treasury Department received no data from the EU for nearly eight months of 2010, pending the negotiations and approval of the Agreement, it had no ability to meaningfully review the data during that period and refine its Requests. After the entry into force of the Agreement and the receipt of data in August 2010, the Treasury Department began anew its comprehensive review, which it completed in January 2011. As a result of that review, it further refined and narrowed its Requests, beginning in February 2011. The Treasury Department will conduct future reviews to ensure the Requests are tailored as narrowly as possible.

9. Has Europol been able to perform its verification function within an appropriate timeframe as required under Article 4 (4)? What has been the average timeframe Europol has required for this verification function?

Europol has performed its verification function within an appropriate timeframe as required under Article 4 (4), which provides that Europol shall verify the Requests "as a matter of urgency". Europol has performed its verification function, on average, within two business days of the completion of the U.S. submission of its Request and supplemental documents (including any additional information requested by Europol).

10. Have there been any cases in which Europol has found that the request under Article 4 (1) did not meet the requirements set out in Article 4 (2)?

Europol has not determined that a Treasury Department Request did not meet the requirements set out in Article 4(2). With respect to two (of the six) Requests that Europol received during the relevant period, however, Europol requested that the Treasury Department supply additional information relating to particular areas of the Request prior to the

verification, and the Treasury Department responded with the additional information requested. As a supplement to the documentation provided, Europol also has requested that the Treasury Department provide periodic briefings to include, among other matters, sensitive and classified information and analyses relating to current terrorism threats in order to fully substantiate the necessity of the data and to demonstrate that the Requests are tailored as narrowly as possible. The Treasury Department has provided two such classified briefings to Europol (one in Washington and the other in The Hague) in the six months since the Agreement entered into force. A third such briefing is scheduled for March 2011 in Washington, D.C.

11. If so, have there been any cases where the request was modified as a consequence of Europol finding that it did not meet the requirements set out in Article 4 (2)?

Europol has not made such a finding.

12. Have any particular issues related to the implementation of the Agreement been identified? If so, which?

No.

13. What is your overall assessment of the effectiveness of the Agreement? Have any specific impediments to achieving the stated purpose of the Agreement been identified? If so, which?

The Treasury Department assesses that the Agreement has been effective in supporting global counter-terrorism efforts and has identified no specific impediments to achieving the stated purpose of the Agreement.

III. Compliance with the data protection obligations specified in the Agreement

14. What measures have been put in place to ensure that provided data shall be processed exclusively for the prevention, investigation, detection, or prosecution of terrorism and its financing?

A comprehensive and overlapping set of systems and controls has been established to ensure that provided data are processed exclusively for the prevention, investigation, detection, or prosecution of terrorism or its financing and that all searches of provided data are based on pre-existing information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing. These systems and controls include the following:

- All analysts who have access to the TFTP system are extensively trained and re-trained regularly to ensure the fulfillment of all requirements for searches, including that a pre-existing nexus to terrorism is documented for every search; if an analyst even attempts a search that does not satisfy the requirements, the Treasury Department responds appropriately, with responses varying from mandating additional training for the analyst to removing access rights to the TFTP and instituting disciplinary proceedings;
- Detailed logs are maintained of all searches made, including the identity of the analyst, date and time of search, the search terms used, and the justification for the

search; these logs are regularly analyzed by outside auditors as part of the regular independent audit of the program;

- Electronic controls (in addition to human review and oversight) have been implemented that prevent analysts from conducting a search without inputting the pre-existing nexus to terrorism;
- Other electronic controls aim to prevent certain technical mistakes, such as inputting an "or" instead of an "and" as a search term, that inadvertently could result in an overly broad search;
- Independent overseers retained by the Designated Provider and the European Commission review searches either as they occur or shortly thereafter, prior to dissemination of any results, to ensure that the counter-terrorism nexus and other safeguards have been satisfied; and
- Independent auditors retained by the Designated Provider evaluate the technical and systemic controls to ensure the integrity of the system and the satisfaction of all the safeguards.

15. What measures have been put in place to ensure that the TFTP does not and shall not involve data mining or any other type of algorithmic or automated profiling or computer filtering?

The systems and controls outlined in response to Question 14, above, prevent any type of data mining or profiling because they require individualized searches, based on an individual's pre-existing nexus to terrorism.

16. What measures have been put in place to implement the provisions of Article 5 (4) on data security and integrity?

Multiple physical and technical security layers exist to ensure data security and integrity. The data are stored in a secure location accessible only by U.S. Government-cleared personnel and in a secure analysis area accessible only by a limited number of TFTP program managers and analysts and security personnel. The data are stored separately from other data, are not interconnected with any other database, and are protected by multiple security layers that prevent unauthorized access to the data. Significant physical and technical security controls exist to ensure that no copies of TFTP data may be made, except for disaster recovery purposes. The independent auditors retained by the Designated Provider review and verify these physical and technical security safeguards.

17. What measures have been put in place to ensure that all searches of provided data are based on pre-existing information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing, other than the measures indicated in Article 12?

Please see response to Question 14, above.

18. Have there been any cases where personal data revealing racial or ethnic origin, political opinions, or religious or other beliefs, trade union membership, or health and sexual life (sensitive data) have been extracted? If so, have any special measures been taken for additional protection of such sensitive data?

The Treasury Department is not aware of any cases in which such data have been extracted.

19. What measures have been put in place to organise the ongoing and at least annual evaluation to identify non-extracted data that are no longer necessary to combat terrorism or its financing? Have such data been deleted since the entry into force of the Agreement?

Please see response to Question 8, above.

20. Have there been any cases where financial payment messaging data were transmitted which were not requested?

No.[6]

21. What measures have been taken to provide for the ongoing and at least annual evaluation to assess the data retention periods specified in Article 6(3) and 6(4) of the Agreement? Have there been any cases where these retention periods have been reduced in accordance with Article 6(5)?

The Treasury Department assesses these data retention periods as part of its regular review, analysis, and audit of data, as described in response to Question 8, above. The Treasury Department continues to find valuable counter-terrorism leads in data retained for the limits of the current retention periods specified in the Agreement and believes the current retention periods to be appropriate.

22. What measures have been put in place to ensure that information extracted from provided data is retained for no longer than necessary for specific investigations or prosecutions for which they are used?

The Treasury Department notifies law enforcement and intelligence agencies that receive leads derived from TFTP data to retain them for a period no longer than necessary for the purpose for which they were shared. Counter-terrorism analysts using the TFTP receive training on the safeguards, dissemination, and retention procedures prior to use of the system.

23. What measures have been put in place to ensure that onward transfer of information extracted from the provided data is limited pursuant to the safeguards laid down in Article 7 of the Agreement?

TFTP-derived information is shared with counter-terrorism, law enforcement, or public security authorities in the United States, EU Member States, third countries, or with Europol or Eurojust for lead purposes only and for the exclusive purpose of the investigation, detection, prevention, or prosecution of terrorism or its financing. Counter-terrorism analysts using the TFTP receive training on the safeguards, dissemination, and retention procedures prior to use of the system. Information is only disseminated after

[6] Certain media reports have alleged that the TFTP received SEPA data despite the provisions of Article 4, which prohibit the Treasury Department from requesting such data pursuant to the Agreement. Such reports are incorrect, a fact publicly confirmed by the Designated Provider. See www.swift.com/news/compliance/misleading_information_SEPA.

approval by management trained on the safeguards identified in the Agreement. Any subsequent dissemination requires the express approval of the Treasury Department.

In cases in which the Treasury Department is aware that TFTP-derived information of a citizen or resident of a Member State is to be shared with a third country, the Treasury Department abides by the existing protocols on information sharing with that Member State. In cases where existing protocols do not exist, the Treasury Department will not disseminate the information without prior consent of the concerned Member State except where the sharing of data is essential for the prevention of an immediate and serious threat to public security.

24. Under what circumstances have the overseers mentioned in Article 12 of the Agreement requested additional information or blocked any searches on the grounds that they appear to be in breach of Article 5 of the Agreement? Under what circumstances has the EU appointed overseer requested additional information or blocked any searches on the grounds indicated above?

The overseers mentioned in Article 12 of the Agreement – one appointed by the European Commission and the others employed by the Designated Provider – routinely request additional information to ascertain strict adherence to the counter-terrorism purpose limitation and other safeguards described in Articles 5 and 6 of the Agreement. The overseers may request additional justification or clarification of the counter-terrorism nexus as well as documentation to ensure that the search is as narrowly tailored as possible. In certain cases, the overseers request additional information simply for routine auditing purposes and not out of any concern with the search itself.

In the six months between August 1, 2010, and January 31, 2011, the overseers queried 304 searches – a large number of which were selected for routine auditing purposes. In the overwhelming majority of these cases (well over 90%), the overseers were fully satisfied with the search as formulated. In a small number of cases, the overseers were not satisfied with the search as formulated. In cases where the searches were queried by the overseers at the time of the search, no results were returned to the analyst unless and until the search terms satisfied the overseers. In cases where the searches were identified through retrospective review, no information obtained through the searches was disseminated or used until the overseers were satisfied.

25. What measures have been taken to ensure that the results of the searches are not disseminated before the overseers have had a chance to review the search?

Any dissemination of TFTP-derived information requires management approval, and subsequent dissemination requires the express approval of the Treasury Department. The Treasury Department trains counter-terrorism analysts on the proper guidelines and standards regarding the dissemination and use of TFTP-derived information. All TFTP analysts have been trained to ensure that there is no dissemination of TFTP-derived information prior to the completion of the overseer review process.

26. Have there been any cases where individuals have sought access, rectification, erasure or blocking in accordance with Article 15 and 16 of the Agreement? If so, how many, and how have these cases been resolved?

The Treasury Department has received one case in which an individual apparently sought to invoke the right of access described in Article 15 of the Agreement. A national data

protection authority ("NDPA") from an EU Member State submitted a request to the Treasury Department, citing Article 15, on behalf of an individual. Because this request did not conform to the customary procedures followed by the Treasury Department and posted on the Treasury Department's public website, the Treasury Department responded to the NDPA and requested certain basic information, pursuant to the Treasury Department procedures, including that the request be signed by the requester and contain confirmation that the requester consents to any personal data being shared with the NDPA. Neither the NDPA nor the requester responded to the Treasury Department.

Another individual sent an email to the Treasury Department inquiring about the relevant procedures to invoke the rights described in Articles 15 and 16. The Treasury Department responded via email outlining the relevant procedures and referring the individual to relevant EU and Treasury Department websites containing additional information on submissions of requests. The individual never responded or submitted any type of request.

No rectification request pursuant to Article 16 has been submitted to date.

27. Have there been any cases where you have become aware that data received or transmitted pursuant to the Agreement were not accurate? If so, what measures have been taken to prevent and discontinue erroneous reliance on such data?

The Treasury Department is not aware of any instance in which data received or transmitted pursuant to the Agreement were inaccurate.

28. Have there been any cases where individuals have made use of the means of redress described in Article 18 of the Agreement? If so, how many, and how have these cases been resolved?

The Treasury Department is not aware of any such cases other than those described in response to Question 26, above.

ANNEX B
COMPOSITION OF THE REVIEW TEAMS

The members of the EU team were:

- Reinhard Priebe, Director Internal Security, Directorate-General Home Affairs – Head of the EU delegation;
- Martin Schieffer, Deputy Head of Unit, Unit A1 - Crisis management and fight against terrorism, Directorate-General Home Affairs;
- Dick Heimans, Head of Sector, Unit A1 - Crisis management and fight against terrorism, Directorate-General Home Affairs;
- Willem Debeuckelaere, expert on data protection from the Belgian data protection authority;
- Paul Breitbarth, expert on data protection from the Dutch data protection authority;
- Carlos Zeyen, judicial expert from Eurojust.

It is noted that Willem Debeuckelaere, Paul Breitbarth and Carlos Zeyen participated in the EU team as experts for the Commission and not in their other professional capacities.

The members of the US team were:

- John E. Smith, Associate Director, Office of Foreign Assets Control, U.S. Department of the Treasury – Head of the delegation;
- Mike J. K. Maher, Jr., Deputy Assistant General Counsel (Enforcement & Intelligence), U.S. Department of the Treasury;
- James Earl, Policy Analyst, Office of Foreign Assets Control, U.S. Department of the Treasury;
- Mary Lee Warren, Senior Counsel for the European Union and International Criminal Law Matters, U.S. Mission to the European Union;
- Nancy C. Libin, Chief Privacy & Civil Liberties Officer, Office of the Deputy Attorney General, U.S. Department of Justice;
- Alexander W. Joel, Civil Liberties Protection Officer, Civil Liberties and Privacy Office, Office of the Director of National Intelligence;
- Roksana Houge, Economic Officer, Office of European Union Affairs, U.S. Department of State.