EUROPEAN
COMMISSION

Brussels, 14.12.2012
SWD(2012) 454 final

COMMISSION STAFF WORKING DOCUMENT

Report on the second 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

October 2012

TABLE OF CONTENTS

1. PROCEDURAL ASPECTS – SCOPE, MANDATE, METHODOLOGY

Following the first joint review in February 2011, which covered the period of the first six months after the entry into force of the Agreement (1 August 2010 until 31 January 2011), the second joint review covered the ensuing period from 1 February 2011 until 30 September 2012. To avoid repetitions as to the background, history and content of the EU-US TFTP Agreement, reference is made to the report on the first review from 30 March 2011.[1]

Pursuant to Article 13(1) of the TFTP Agreement, the joint review should cover *"the safeguards, controls, and reciprocity provisions*" set out in the Agreement. In this context, Article 13(2) specifies that the joint review should have particular regard to:

(a) The number of financial payment messages accessed;

(b) The number of occasions on which leads have been shared with Member States, third countries, and Europol and Eurojust;

(c) The implementation and effectiveness of the Agreement, including the suitability of the mechanism for the transfer of information;

(d) Cases in which information has been used for the prevention, investigation, detection, or prosecution of terrorism or its financing;

(e) Compliance with the data protection obligations specified in the Agreement.

Article 13(2) further states that "*the review shall include a representative and random sample of searches in order to verify compliance with the safeguards and controls set out in this Agreement, as well as a proportionality assessment of the Provided Data, based on the value of such data for the investigation, prevention, detection, or prosecution of terrorism or its financing.*"

The second review was conducted jointly by a US review team and an EU one. According to Article 13(3), the Commission represents the EU in the joint reviews. Consequently the EU review team was headed by a senior Commission official and, in total, consisted of three members of Commission staff and three external experts, namely two data protection experts and an expert with judicial experience, who supported the Commission in reviewing the agreement, in accordance with Article 13(3). A list of the members of both review teams, EU and US, appears in Annex I.

As to its schedule, the second joint review was carried out in two main steps: on 4 October 2012 in The Hague at Europol premises and on 30 and 31 October 2012 in Washington at the U.S. Treasury Department (hereinafter "the Treasury"). The following methodology was applied:

– Both review teams first met in The Hague at Europol's headquarters and were informed by Europol senior staff and experts on Europol's implementation and practical application of the Agreement. The teams visited the secure location where

[1] SEC(2011) 438 final.

Europol handles the US requests and met the persons having access to the data in question.

– To prepare the visit in Washington, the EU team had sent a questionnaire to the Treasury in advance of the review. This questionnaire contained specific questions in relation to all the aspects of the review as specified in the Agreement. The Treasury provided written replies to the questionnaire (Annex II). The EU review team also posed further questions to Treasury officials and was able to address all the various parameters of the Agreement.

– The review teams were granted access to relevant Treasury premises, including the site where the TFTP is operated. For security reasons, review team members were required to provide advance evidence of their security clearances to access the TFTP facility.

– The review teams were 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 US confidentiality requirements.

– The review teams had direct exchanges with Treasury personnel responsible for the TFTP program, the overseers who review the searches of the data provided under the TFTP Agreement, and the full-time auditor of the TFTP employed by the Designated Provider.

– The review teams did not carry out any system checks or controls on the basis of log files.

This report is based on information contained in the written replies that the Treasury provided to the EU questionnaire, information obtained from the discussions with Treasury personnel as well as information contained in other publicly available Treasury documents. In addition, information provided by Europol staff, both orally and in writing, was used and the findings in the two inspection reports of Europol's Joint Supervisory Body (JSB) from March 2011 and March 2012 were taken into account. Finally, the Commission's replies to 15 questions posed by Members of European Parliament[2] were considered and, to complete and/or confirm the information available to it, the Commission also met occasionally with the Designated Provider and held a classified meeting with Member States on the application of Article 10 of the Agreement.

Due to the sensitive nature of the TFTP, there were limitations on the provision of some documents during the review. Some information was provided to the review teams 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 consultation and reading in the Treasury premises. The review itself was conducted over a period of three days ("1+2"), with additional briefings and review activities occurring 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, following a request from the Treasury, all members of the review teams had to sign non-disclosure agreements

[2] E-11200/2010; E-2166/2011; E-2762/2011; E-2783/2011; E-3148/2011; E-3778/2011; E-3779/2011; E-4483/2011; E-6633/2011; E-8044/2011; E-8752/2011; E-617/2012; E-2349/2012; E-3325/2012; E-7570/2012.

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

Given its timing just 6 months after the entry into force of the agreement, the first review concentrated on whether all the mechanisms of the Agreement had been put in place. The second review was able to look more in depth into whether the Agreement was functioning well. This included verifying its further implementation and the continued proper functioning of the mechanisms contained in it. Due to the longer period of implementation and application that was under review, this time the EU review team was in a position to look at more data gathered over a longer period which helped it to substantiate its view regarding the effectiveness and practical use of the Agreement, both for the US in obtaining security related information in the framework of the TFTP as well as for the EU in return receiving information from possible findings under this programme. The review also considered whether the recommendations made in the first review report had been followed up.

The second review was based on the understanding that it was not its task to provide a political judgement on the Agreement, this being considered outside the scope and mandate under Article 13. The focus of this report is therefore to present the review's findings in a manner which is as objective as possible. Where recommendations are presented, these are aimed at further increasing the effectiveness of the application of the Agreement, in particular its safeguards.

Before, during, and after the review there has been an exchange of views in an open and constructive spirit which covered all the questions of the review teams. Therefore the Commission would like to acknowledge the good cooperation on the part of all Treasury and other US personnel, personnel of Europol and the Designated Provider, as well as the EU-appointed overseers during the review, and expresses its gratitude for the way in which the questions of the review teams have been replied to.

Finally it should be clarified that this report was prepared by, and reflects the views of, the EU review team, based on the work of the joint review and other work independently conducted on the EU side. However the modalities for the second review and the procedure for the issuance of this report were agreed with the Treasury, including an opportunity for the latter to conduct a prior check of this report for the purpose of identifying any classified or sensitive information that could not be disclosed to the public.

2. THE OUTCOME OF THE SECOND JOINT REVIEW

2.1. Findings

2.1.1. Statistical information

The issue of the overall volume of financial payment messages provided to the Treasury under the Agreement has been central to discussions on statistics. While this aspect is not explicitly referred to in Article 13 of the Agreement as an obligatory element of the review, it is obvious that there is an interest to be informed on this point in order to fully understand the scope of the programme, its possible implications for civil liberties, and thus its proportionality. As during the first review, the US side did not disclose concrete figures on

data volumes, reconfirming its view that revealing too detailed information on data volumes would in fact provide indications as to the message types and geographical regions sought (in combination with other publicly available information) and would lead to the effect that terrorists would try to avoid such message types in those regions. However the US side expressed understanding for the EU interest in data volumes and agreed to provide at least trends which give some indications on the actual overall amount of data transferred to the US. These trends show a continuous decrease from the previous to this reporting period.

In comparison to the previous reporting period, also the number of searches that were performed on those data went down significantly. During the 20 months of the period under review, TFTP analysts conducted 31 797 searches in the TFTP, an average of 1 590 searches per month. This number includes searches involving data stored in and 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, according to the Treasury, involve neither the EU nor its residents.

There is no clear-cut explanation for these decreases. One possible reason could be a backlog before the first reporting period due to the (temporary) lack of an agreement as a basis for data exchange before the adoption of the EU US TFTP Agreement. Another reason could be the Treasury decisions, as part of its on-going utility-based reviews of the data, to narrow the message types responsive to its requests on three separate occasions during the period under review – in February 2011, September 2011, and October 2011 as referred to in the responses to the EU questionnaire (see Annex II).

Assessing the added value of the TFTP and communicating clearly and openly about the implementation of the programme and the Agreement can only be done in so far as this does not jeopardise the on-going value and integrity of the programme. The Treasury has on many occasions expressed its concern to ensure that no sensitive or classified details of the programme should become public as this could harm the effectiveness of the programme. This concern was also demonstrated by the procedures on security clearances and the non-disclosure agreements which the members of the review teams were asked to sign. This is an understandable concern, given the importance of the programme for preventing and combating terrorism and its financing. Information on the functioning of the programme should not be provided at the risk that this information might be misused by those being fought by it.

The resulting need for confidentiality necessarily limits the possibilities for this report to communicate some details on the implementation of the Agreement. On the other hand there is a clear interest for substantial information to assess the necessity of providing data for TFTP. Two examples of the tension this can create were discussed in particular by the review teams – the overall volume of financial payment messages provided under the Agreement to US authorities, and the number of searches which were performed on this data. Generally, the second review tried to strike a balance in that US confidentiality requirements have been strictly followed in order to enable the Treasury to provide to the review teams relevant classified information.

2.1.2. Requests to obtain data from the Designated Provider – the role of Europol

The requests under Article 4 were received, on average, every month, and covered a period of four weeks. During the period under review Europol received 21 requests from the Treasury. In three cases Europol asked the US side for supplemental information which it then received. Europol issued a delay notification to the Designated Provider on one occasion because the verification process was expected to take longer than 48 hours of working days. In no cases did the verification lead to a rejection of the request. The statistical information provided by Europol to the review teams is attached as Annex III.

Both Europol and the Treasury explained that no SEPA data[3] has been requested or transmitted which was also confirmed by the Designated Provider.

The Treasury explained its processes for updating and revising the supplemental documents provided to Europol in connection with each Article 4 verification request. Taking into consideration the most recent terrorist threats and vulnerabilities, counter-terrorism analysts assess the scope of the request and update the supplemental documents for Europol to include recent specific and concrete examples of terrorist threats and vulnerabilities, as well as the uses of TFTP data, and how they relate to the request. Treasury policy staff then provides relevant policy updates and review the documents for accuracy and completeness. Next, the Treasury counsel conducts a thorough legal review to ensure that the request, including the supplemental documents, complies with the criteria of Article 4. Finally, the Director of the Treasury Department's Office of Foreign Assets Control reviews the documents and confirms that the Article 4 standards are satisfied and that the request reflects current counter-terrorism reports and analyses.

The Treasury explained that this process of updating and reviewing the supplemental document is considerably work intensive. The constant updating and refining have caused the documents provided to Europol to grow from 51 pages in August 2010, when the Agreement entered into force; to 63 pages in February 2011, the month of the first joint review; to 104 pages in September 2012, the end of the period now under review. The review teams had the opportunity to examine two examples of the classified supplemental documents provided to Europol by the Treasury as part of the Article 4 process and to discuss on that basis the procedures for handling and the scope of the requests. The examples examined dated from, respectively, the beginning and the end of the reporting period and the review teams noted the increased information contained therein – much of it in response to direct requests from Europol and following up some of the recommendations made to Europol by its JSB, especially as concerns sufficient information in writing. The EU review team believes that cooperation between Europol and the Treasury has resulted in substantial improvements to the Article 4 process and is satisfied that this process is proceeding in compliance with the Agreement.

During the period under review Europol has shown that it has taken seriously the criticism and calls for improvements expressed by various stakeholders. It has worked to follow these recommendations and apply them in the applicable counter terrorism context. In 2011 Europol

[3] For more information on what is to be understood by SEPA data (formats), see the website of the European Payment Council (http://www.europeanpaymentscouncil.eu) and the reply of the Commission to written question E-7516/2010.

held a number of workshops with the JSB to improve the verification mechanism which, at one occasion, also involved Treasury experts. This cooperation, as well as the present joint review, has allowed some possible misperceptions on the nature and the scope of the Article 4 mechanism and on how it is applied in practice to be eliminated.

Europol explained to the review teams that it carries out its verification task under Article 4 based on an *operational* assessment of the validity of the US request, within the general context of its robust data protection framework and involving also closely Europol´s data protection officer (DPO) and its legal department. The fact that the verification task under Article 4 has been given to Europol, i.e. to a law enforcement and not to a data protection body, shows that, ultimately, the verification criteria set out in Article 4 have to be assessed in the light of operational considerations and security needs. This is particularly true for the difficult question whether the US requests are "*as narrowly tailored as possible*" (Article 4 (2) lit. c). The final responsibility for this operational assessment lies solely with Europol which enjoys a margin of discretion when deciding on this specific requirement. Consequently the review teams felt that it is not for them (nor for any other monitoring body) to replace Europol´s final decision by their own less informed judgement. In this context it is also important to note that Europol´s DPO explicitly confirmed that Europol has not taken any positive verification decision against his advice.

Based on the explanations and information provided by Europol and the Treasury during the review, it can be concluded that the application of Article 4 has now reached an entirely satisfactory level, and that Europol is fully accomplishing its tasks pursuant to Article 4.

It is recommended that

– the Treasury continues to make requests (together with any supplemental documents) with detailed and regularly updated justification as currently provided, and

– Europol continues to carry out its tasks pursuant to Article 4 following the high verification standards currently agreed upon.

2.1.3. Monitoring safeguards and controls – the role of the overseers

Article 5 provides for safeguards to ensure that the provided data is only accessed in cases where there is a clear nexus to terrorism or its financing, and where the search of the data is narrowly tailored. The 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 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 US authorities will thus not produce any noticeable effect on the persons whose data is provided but not accessed.

The review teams verified that the safeguards described in Article 5 have indeed been put into place and function as intended. In addition, the review teams specifically looked at the oversight mechanism described in Article 12, and on how this affects the effectiveness of these safeguards.

Technical provisions have been put in place, which aim at ensuring that no search can take place without the entry of information on the terrorism nexus of the search. The review team is satisfied that data is processed exclusively for the purpose of preventing, investigating, detecting or prosecuting terrorism or its financing (Article 5 (2)). This is also confirmed by the examples of cases in Annex IV.

The joint review team saw a practical demonstration of a search at the Treasury. The analysts operating the searches demonstrated that specific measures have been taken with the objective that the searches are tailored as narrowly as possible by meeting both operational and data protection considerations. The Treasury expressed the view that the operational effectiveness of the system would be reduced by searches which are not narrowly tailored, since these would return too many results and thus too much irrelevant data.

The respect of these safeguards is ensured through the work of independent overseers, as referred to in Article 12. This specific mechanism of control has been further enhanced during the reporting period. By the date of entry into force of the Agreement and in order to guarantee an immediate take-up of that function, the Commission had recruited an overseer on a temporary basis to accomplish the tasks of the EU overseer. Subsequently, following the usual applicable recruiting process for EU officials and agreement of the Treasury, the permanent EU overseer was able to take post in May 2011. He underwent intensive training on the job, established contacts with the other independent overseers recruited by the Designated Provider, participated in relevant Treasury security briefings and reported regularly back to the Commission. Moreover, the Treasury has put in place arrangements to facilitate the exercise of his functions and to ensure that he can fulfil his tasks in an effective way.

Despite the general satisfaction with the implementation of the Agreement and its safeguards, during the period under review, it became obvious that the safeguard represented by the EU overseer could be further improved and strengthened. The work as an EU overseer is a technical and demanding activity which should not be performed by just one person on a daily full-time basis. In addition, holiday periods and absences due to sickness rendered it advisable to reinforce the EU overseer function by recruiting a second person. Given that the team of overseers recruited by the Designated Provider consists of three part-time overseers and one full-time post, reinforcing the EU side of the independent overseer mechanism better reflects the EU's recognition of the importance of this task for the correct, effective and continued implementation of the Agreement.

Consequently, it was agreed to strengthen the role of the EU overseer by recruiting a deputy EU overseer. The US agreed to the Commission’s request to add this position to the safeguards already in place and to have it also located directly at the Treasury which is beyond what is required by the Agreement. Following a formal recruitment procedure the deputy was selected and had taken up duty in Washington when the review teams had their on-site visit.

The review teams had the opportunity to speak to the most senior of the overseers recruited by the Designated Provider, as well as to the EU overseer and his deputy. The review teams were 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 overseer appointed by the EU, had initiated the blocking of searches to request additional information. The review teams recognised that due to US security clearance reasons, there have been certain limits for the EU overseer to see some data. This, however, did not prevent the necessary control as envisaged by the Agreement as the joint review team was informed that the overseers work in a complementary way by supporting each other in order to accomplish their tasks. With the deputy EU overseer being operative and complying with the highest US security clearance standards, this successful co-operation will be further enhanced. The overseers perform real-time and retrospective reviews. It was confirmed to the review teams that even in cases of retrospective review the Treasury does not disseminate any data before notification by the overseers. The EU overseer reported that he also sees all requests from Member States sent via Europol.

The mechanism of the overseers has been further developed and is now well established. There are no indications that the requirements laid down in Article 6 (no dissemination before notification) have not been met.

It is recommended that

– the overseers recruited by the Designated Provider and the EU overseers continue to carry out their supervisory tasks in a complementary way, and

– the EU deputy overseer quickly becomes fully operational and integrates into the team of overseers.

2.1.4. Data security and integrity – independent audit

The EU review team had the opportunity to visit the premises in the Treasury where TFTP-related searches are carried out and data is handled. In addition, questions related to this issue in the questionnaire – as well as raised orally in the course of the on-site visit – were replied to comprehensively and convincingly by the Treasury. Finally, the EU review team had the opportunity to speak to a representative of the Designated Provider responsible for auditing procedures to test data security and integrity. He provided a detailed presentation and replied to subsequent questions raised by the team. Based on all this, the EU review team considers the measures taken to ensure data security and integrity as adequate. Utmost care has been and is being taken by the US 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, and that the provided data shall not and even cannot be subject to any manipulation, alteration or addition as the Designated Provider or the issuing bank would be the only ones having the actual capability to do so. In addition, it became clear that no copies of provided data would be made, other than for recovery back-up purposes. The independent auditors' representative, who monitors the implementation of these safeguards on a daily basis, confirmed that they execute regular security tests related amongst others to application, physical, logistical, network and database security. These auditors report back to the Designated Provider every three months including on the fact whether there have been any discrepancies or atypical occurrences related to the data traffic.

Following these thorough explanations, it can be concluded that Article 5 has been implemented appropriately.

2.1.5. Data protection

Data protection related to the TFTP is essential and consequently has been addressed in detail in the EU US TFTP Agreement. The most relevant Articles in this context are Articles 6, 14, 15 and 16, as well as Article 18. Given the sensitivity of data protection and the TFTP, the Agreement requires that the EU review team contains two data protection experts from Member States. Specific reference is made to the Annex II of this report containing the Treasury responses to the EU questionnaire which complements the findings below.

2.1.5.1. Retention and deletion

Pursuant to Article 6, the first deletion of data should have taken place not later than by 20 July 2012. The EU review team was satisfied to learn from the Treasury that this deadline was met for the relevant data. This was confirmed by the auditors of the Designated Provider. The Treasury explained the practical challenge that this exercise (the hard deletion of all non-extracted data for the set timeframe from the database) represented to them due to the technical complexity of the system, the need to ensure strict compliance with the Agreement's safeguards and the danger of causing any accidental harm to the functioning of the whole system as well as on data not yet designated for deletion. Based on the experience with this complex exercise the Treasury informed the EU review team that the deletion of data cannot be implemented as an on-going process (on a rolling basis) but that their intention would be to carry out this complex and complicated exercise only after longer time intervals. Following the review, the Treasury provided assurances that, going forward, measures will be taken to ensure that all non-extracted data will be deleted no later than 5 years from receipt. To this end, the Treasury informed the Commission that it has begun the process of deleting all non-extracted data received between 20 July 2007 and 20 July 2008, and that it expects this process to be completed by February 2013.

Article 6(5) requires the Treasury to undertake an on-going and at least annual evaluation to assess the data retention periods specified in Article 6(3) and (4) to ensure that they continue to be no longer than necessary to combat terrorism or its financing. At the review the Treasury reaffirmed without further specifications that this evaluation is carried out in practice.

Article 6(6) requires the Commission and the Treasury to prepare a joint report regarding the value of TFTP Provided Data not later than three years from the date of entry into force of the Agreement.

It is recommended that – the Treasury specifies more in detail to the Commission how the on-going evaluation process addressed in Article 6(5) is carried out in practice, and – the practice of deletion of data pursuant to Article 6 and its paragraph 4 in particular is monitored continuously and further addressed in the report pursuant to Article 6(6).

2.1.5.2. Providing information to the data subject

As required by Article 14, 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.

Apart from the website, the Treasury also has an e-mail service available, as well as a telephone hotline. The telephone hotline 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. The EU review team was given a demonstration on how this works in practice. The Treasury confirmed that its personnel will call back the individual, if possible, within 24 hours. During the review period, 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 EU review team welcomes the Treasury's practice of recording voicemail messages as this provides better safeguards for accountability.

During the review period, the specific e-mail account set up by the Treasury to answer questions on TFTP (tftp@treasury.gov) has only been used five times, by three different individuals. Treasury personnel responded to all such e-mails with appropriate information.

2.1.5.3. Right of access

Upon the entry into force of the Agreement, the Treasury set up the procedures for individuals to seek access to their personal data under the TFTP Agreement. This procedure was described in detail in the first joint review report and can also be found on the Treasury website. It has to comply with US national law as well as the Agreement.

The issue of how individuals sending requests for access identify themselves to the US authorities was addressed in the report on the first joint review. Work on a uniform procedure and common templates to facilitate this identification process and to avoid the need for distributing additional personal data to the Treasury for such a request, is about to be finished with a view to their application as of 2013. On the EU side, all contributions to this important exercise, including those from the Advisory Group established under Article 29 of the Data Protection Directive 95/46/EC (Article 29 Working Party) have been channelled through the Commission as it is responsible for monitoring the implementation of the Agreement.

During the review period, no access requests from individuals meeting the procedural requirements of the Agreement have been received by the Treasury, neither directly nor through an national Data Protection Authority.

2.1.5.4. Right to rectification, erasure or blocking

The procedures to exercise the rights to rectification, erasure or blocking are similar to the procedure 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.

In order to ensure the integrity of the database, as stipulated by Article 5(4)(d), the data provided under the Agreement cannot be changed or altered. 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 be flagged to indicate that such data can no longer be relied upon.

In its first report the EU review team recommended 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. The Treasury confirmed that an up-date of the relevant website had taken place, including the section with frequently asked questions and they provided copies thereof. The EU review team checked this explanation and was satisfied to see that the procedure for how to claim these rights is clearly explained on the website. However, it does not follow from the current version of the frequently asked questions that a rectification of data in the strict sense is technically not feasible and that the only possibility would be to flag the data as being erroneous.

It is recommended that – information on the Treasury website referring to the right of rectification of data explains what a rectification means in this context due to technical constraints, and – the Treasury continues to up-date the website regularly, where necessary, with the support of the Commission.

2.1.5.5. Redress

Under Article 18, individuals have several possibilities for redress, both under European law and under US law. The US redress mechanism was described in detail in the report on the first joint review. The European redress mechanism follows general EU and Member State redress provisions. In the period under review, there was not one single case of a claim for redress addressed to the US, nor is the EU review team aware of any such case in the EU.

2.1.6. Reciprocity – the EU benefiting from TFTP data

Reciprocity is a basic principle underlying the Agreement and two provisions (Articles 9 and 10) are the basis for Member States as well as, where appropriate, Europol and Eurojust to benefit from TFTP data. These provisions enable EU authorities to obtain directly relevant financial data from the Treasury which helps them to fight terrorism and its financing more efficiently in the EU. Consequently, the application of the reciprocity clauses is essential for the EU and its Member States to benefit directly from the data transfer in order to enhance security in the EU.

Pursuant to Article 9, the Treasury Department shall ensure the availability to law enforcement, public security, or counter terrorism authorities of concerned Member States, and, as appropriate, to Europol and Eurojust of information obtained through the TFTP. Article 10 stipulates that a law enforcement, public security, or counter terrorism authority of a Member State, or Europol or Eurojust, may request a search for relevant information obtained through the TFTP from the US if it determines that there is reason to believe that a person or entity has a nexus to terrorism or its financing. During the initial phase of the agreement, Member States made only limited use of this mechanism. Recently, however, this situation changed as Europol figures and information provided by Member States showed.

There were only fifteen Article 10 requests during the six-month period covered by the first review report but 94 such requests in the period currently under review. One reason for this increase is greater awareness of this mechanism on the part of Member States. Europol actively contributed to raising this awareness by promoting the reciprocity provisions through dedicated campaigns in Member States.

The majority of these requests originated from individual Member States, some of them originated from Europol, and two from Eurojust. Article 10 also provides for Member States to contact the Treasury directly without the need to inform Europol of such a request, although this procedural way was not utilised during the review period. A recent meeting with Member States' law enforcement experts showed that the total figure of Article 10 requests is slightly higher than that given above, as a few requests were not provided to the Treasury by Europol due to an insufficient counter-terrorism nexus. In this context it is important to note that all requests from EU authorities for searches in the TFTP must meet the requirements of Article 10.

The Treasury provided figures on the number of "leads"[4] pursuant to Article 10. In addition, it was of the view that existing bilateral protocols on information sharing with certain Member States could be seen as the applicable legal basis for such data exchange, as referred to in the last recital of the agreement's preamble.

The EU review team learned from the EU overseer that he sees the direct requests from Member States without being informed on the identity of the originating Member State. Given this direct channel that the Agreement allows for, it is important that the safeguards of Article 5 (to which Article 10 refers) are complied with also in these cases. In order to apply the safeguards, it appears indispensable that more coordination is done in this respect within the EU. In addition, it would be useful if Europol was at least informed by Member States on their direct requests under Article 10 in order to enhance Europol's analytical capacities to the benefit of the EU as a whole. To support Member States to channel requests for TFTP searches, Europol has set up a single point of contact (SPOC) and with its Analysis Work File (AWF) environment and well established cooperation with the Treasury, it is best placed to handle Member State requests effectively, check them against the Article 5 safeguards, cross-match them against existing databases and further disseminate any lead, where appropriate and with the agreement of the data owner. Moreover a strong single point of contact function would enable Europol to collect information necessary to provide an EU wide overview of terrorist threats and activity. The EU review team is aware that the Agreement does not contain any obligations for Member States to proceed through Europol and that they continue to be able to submit requests for TFTP searches directly to the Treasury. However, in order to improve the EU's response to terrorism and its financing and to control the application of the Agreement's safeguards, it would be very useful to have Europol as the EU's single contact point or, where requests are directly submitted to the Treasury, to have the Member States inform Europol of such requests in a systematic and timely manner, at least in all those cases in which the request is generated by law enforcement authorities.

The figures provided to the review teams on the data exchange based on Article 9 were relatively small. The Treasury reported that in the period under review US investigators

[4] As regards the definition of this term used by the Treasury, see Annex II (reply to question 4).

supplied 267 TFTP-derived "reports"[5] pursuant to Article 9 of the Agreement. In June 2011, there was a significantly higher number of Article 9 reports due to the Breivik case in Norway which Europol analysed with regard to possible effects or implications on Member States and the EU. The EU review team assumes that the majority of the exchanges based on Article 9 are also carried out by direct contacts between individual Member State authorities and the US, without involvement of Europol. Such involvement, however, would be extremely desirable for the reasons given above.

The functioning of reciprocity under the Agreement is an essential factor in assessing the necessity for a possible establishment of an equivalent EU system. In this context, Article 11 of the Agreement states that, during the course of the Agreement, the Commission will carry out a study into the possible introduction of an equivalent EU system. In its Decision of 13 July 2010 on the conclusion of the Agreement, the Council invited the Commission to present within three years from the date of entry into force of the Agreement a report of progress on the development of the equivalent EU system with regard to Article 11 of the Agreement. Since autumn 2010, the Commission has worked on the possible introduction in the EU of a system equivalent to the TFTP (European Terrorist Finance Tracking System/EU-TFTS). Following the launch of an impact assessment study, the Commission published a Communication in July 2011 setting out the most realistic options for the way forward. While reactions to this Communication were limited, some Members of the European Parliament took the view that the options tabled were insufficient as they did not encompass a mere data extraction model. To take account of these comments, the Commission expanded its impact assessment by adding extraction options for an EU-TFTS. The work on the impact assessment study also included bilateral meetings between the contractor of that study and US experts. It has turned out that the further information provided by the Treasury and Europol in the course of the review constitutes useful and important input for the completion of the Commission's impact assessment and the subsequent decision on the possible establishment of an EU system. The Commission will in due course report to the European Parliament and the Council on the outcome of the impact assessment and on the feasibility of an EU-TFTS. There will continue to be close cooperation and consultation with the US authorities on this issue, as laid down in Article 11 of the Agreement.

It is recommended that

- to the extent possible in law enforcement contexts, Member States and, where relevant, Eurojust regard Europol as the EU's single reference point for Article 10 requests, and

- that, in all law enforcement cases in which requests are submitted directly to the Treasury, Member States inform Europol of such requests in a systematic and timely manner.

2.1.7. The value of the Agreement – explaining its security benefits through greater transparency

In the course of the second review, the US authorities reiterated their firm commitment to the Agreement and its implementation. They confirmed their view that the TFTP yields great

[5] As regards the definition of this term used by the Treasury see Annex II, reply to question 4.

benefits in assisting the efforts of the European Union, the United States, and their allies to thwart terrorists and increase global security. This was re-confirmed at all levels, from the analysts performing the searches on the database to the highest levels of policy development.

However more efforts are necessary to better explain the added value of the Agreement and in particular its important contribution to rendering people's lives more secure by fighting and preventing terrorism and its financing. These explanations would obviously need to take full account of the fact that the more details of the programme, its functioning and efficiency are made public, the easier it will be for those tackled by the programme to circumvent it. Transparency in this context consequently cannot mean the unlimited disclosure of each and every detail regarding the functioning of the programme.

The Treasury showed understanding for the concerns expressed by the EU review team in this regard. Consequently, they provided the joint review not only with indications of the value of TFTP derived from information on counter-terrorism investigations, but also arranged for the presentation of useful (classified) samples of recent examples for terrorist cases around the world in which TFTP-related information played a decisive role. They explained how that information was analysed and often helped to initiate law enforcement investigations or prevent attacks. This confirmed the value added of the Agreement for enhancing security in the US, the EU and beyond.

The increased use of the reciprocity clauses contained in the Agreement prove that Europol and Member States have become increasingly aware of the value of TFTP data for their task to fight and prevent terrorism and its financing in the EU.

A particular striking example examined during the review is the Breivik case where TFTP-based information helped Norwegian and other European investigators including Europol to identify within hours the channels through which Breivik collected and moved the funds that he used for the preparation of his brutal attacks. The more knowledge is gained on the financial patterns of such terrorists ("lone wolves"), the better are law enforcement and other authorities prepared to understand the thinking of such individuals and ultimately to prevent similar attacks. Based on the TFTP data collected in context of the Breivik case, the Finnish authorities were able to arrest a person pursuing similar terrorist objectives before that person was able to put them in practice.

The cases referred to in Annex IV further illustrate the value of the Agreement and its necessity for combating and preventing terrorism or its financing.

2.2. Ensuring an efficient and effective review

Given the sensitivity of the subject, a regular review of the Agreement is key to ensure its proper implementation, to build up a trustful relationship between the contracting parties and to provide reassurances to interested stakeholders on the usefulness of the TFTP instrument.

The review mechanism is central for achieving those objectives. It has been particularly carefully designed by the Parties as to the substance of the review process, to the cooperation of the review teams and to the process to be followed. The Commission, responsible for the review on the EU side, welcomes any input from EU institutions and actors, Member States and other stakeholders to enable it to carry out the review in the best way possible. Parallel or

uncoordinated initiatives or inquiries should be avoided because they undermine the Article 13 review process and have caused a considerable workload to the Treasury in particular.

Since the entry into force of the Agreement, the Commission and the Treasury have been in constant regular contact on various issues related to the implementation of the Agreement. Also, in relation to its specific tasks, Europol staff has established an intensive dialogue with their Treasury counterparts. This has turned out to be a very important monitoring element, in addition to the formal regular reviews under Article 13.

Proper data protection pursuant to the specific rules laid down in the Agreement is essential for its implementation. This is why Article 13 requires the participation of data protection experts in the review, thus ensuring that the specific data protection safeguards are carefully looked into. Where these safeguards are also monitored by other bodies having responsibilities with regard to the Agreement, their activities should by no means affect the proper functioning of the Article 13 review mechanism.

Regarding the particular duties to be carried out by Europol under the Agreement (Articles 4, 9, 10), the general Europol governance arrangements apply. This includes the supervision by the Management Board and – in relation to handling personal data – by the JSB. During the review, as on previous occasions, the Treasury expressed serious concerns and legal doubts about how the JSB has carried out TFTP-related inspections and communicated on those inspections[6]. This relates in particular to the JSB's decision from mid-October 2012 to grant access to its classified second inspection report to members of European Parliament's LIBE committee without Europol`s and the Treasury's prior consultation and consent, which is considered a clear violation of applicable security rules and a breach of mutual trust.

It is recommended that

– any technical modalities and security arrangements agreed upon with the Treasury for the transfer of information are respected, which includes seeking prior consent from the data owner before disseminating such information;

– in the future, a consultation and coordination takes place between JSB (notwithstanding its independent status), Europol and the Commission on the planning, timing and focus of possible inspections aside the Article 13 review proper in order to avoid overlapping activities and misleading public statements.

3. RECOMMENDATIONS AND CONCLUSION

Based on the findings addressed above, the EU review team is satisfied that the recommendations presented in the report of March 2011 on the first Joint Review have to a large extent been followed up, thus improving the implementation of the Agreement. Providing more verifiable insights into the actual added value of the TFTP, preferably by public information without endangering the effectiveness of this instrument and whilst respecting the need for confidentiality of the methods and procedures used, remains a

[6] The Treasury expressed further these concerns in a letter addressed to the Commission on 16.11.2012.

challenge. As already stated in the first report, transparency on the added value of the programme for the fight against terrorism would go a long way in convincing a wider audience of the real benefits of the TFTP and the Agreement and would raise the level of trust towards the programme, and that such transparency should be sought wherever possible without endangering the effectiveness of the programme as such.

The EU review team is of the opinion that the review mechanism is a valuable tool for the assessment of the implementation of the Agreement and the safeguards included therein. Taking into account the longer period of application of the Agreement this second review indeed allowed a much deeper insight into the functioning of the TFTP. As illustrated by the report (and the detailed information contained in its annexes), this review confirmed the clear value added of this instrument in fighting against and preventing terrorism. This – very sensitive – programme continues to be well protected and is scrupulously managed in accordance with a set of effective safeguards.

The EU review team has noted further improvements of the verification and oversight mechanisms in particular, some of which go beyond what is required in the Agreement. Overall the implementation of the agreement more than two years after the entry into force of the Agreement has reached a very satisfactory level of effective implementation with also the EU increasingly profiting from it under the specific reciprocity arrangements.

To further enhance the quality of the implementation of the Agreement, the EU review team presents the following recommendations:

(1) It is recommended that the Treasury continues to make requests (together with any supplemental documents) with detailed and regularly updated justification as currently provided, and that Europol continues to carry out its tasks pursuant to Article 4 following the high verification standards currently agreed upon (2.1.2).

(2) It is recommended that the overseers of the Designated Provider and the EU overseers continue to carry out their supervisory tasks in a complementary way, and that the EU deputy overseer quickly becomes fully operational and integrates into the team of overseers (2.1.3).

(3) It is recommended that the Treasury specifies more in detail to the Commission how the on-going evaluation process addressed in Article 6(5) is carried out in practice, and that the practice of deletion of data pursuant to Article 6(4) in particular is monitored continuously and further addressed in the report referred to in Article 6(6) (2.1.5.1).

(4) It is recommended that information on the Treasury website referring to the right of rectification of data explains what a rectification means in this context due to technical constraints, and that the Treasury continues to up-date the website regularly, where necessary, with the support of the Commission (2.1.5.4).

(5) It is recommended that, to the extent possible in law enforcement contexts, Member States and, where relevant, Eurojust regard Europol as the EU's single reference point for Article 10 requests, and that, in all law enforcement cases in which requests are submitted directly to the Treasury, Member States inform Europol of such requests in a systematic and timely manner (2.1.6).

(6) It is recommended that any technical modalities and security arrangements agreed upon with the Treasury for the transfer of information are respected, which includes seeking prior consent from the data owner before disseminating such information, and that in the future, a consultation and coordination takes place between JSB (notwithstanding its independent status), Europol and the Commission on the planning, timing and focus of possible inspections aside the Article 13 review proper in order to avoid overlapping activities and misleading public statements (2.2).

According to Article 6(6) of the Agreement, the Commission and the Treasury shall prepare a joint report regarding the value of TFTP provided data no later than three years from the date of entry into force of the Agreement (1.8.2013). Until the same date, the Commission will present a report of progress on the development of an equivalent EU system with regard to Article 11 of the Agreement, as invited by the Council. It has also been agreed that the next Joint Review according to Article 13 of the Agreement will be carried out in 2014.

ANNEX I

COMPOSITION OF THE REVIEW TEAMS

The members of the **EU team** were:

– Reinhard Priebe, Director Internal Security, Directorate-General Home Affairs, European Commission – Head of the EU delegation;

– Martin Schieffer, Deputy Head of Unit, Unit A1 - Crisis management and fight against terrorism, Directorate-General Home Affairs, European Commission;

– Ingo Weustenfeld, Unit A1 - Crisis management and fight against terrorism, Directorate-General Home Affairs, European Commission;

– Dieter Verhaeghe, 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 Dieter Verhaeghe, 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;

– James Earl, Policy Analyst, Office of Foreign Assets Control, U.S. Department of the Treasury;

– M. William Schisa, Attorney Advisor, U.S. Department of the Treasury;

– Alexander W. Joel, Civil Liberties Officer, Civil Liberties and Privacy Office, Office of the Director of National Intelligence;

– Jocelyn A. Aqua, Counsel, National Security Division, Privacy & Data Protection, U.S. Department of Justice;

– Stewart C. Robinson, Senior Counsel for the European Union and International Criminal Law Matters, U.S. Mission to the European Union;

– Leslie Freriksen, Economic Officer, Office of European Union Affairs, U.S. Department of State.

ANNEX II

U.S. TREASURY DEPARTMENT RESPONSE TO THE EU QUESTIONNAIRE

The U.S. Department of the Treasury ("Treasury Department") received the following questionnaire from the European Commission ("Commission") on behalf of the European Union ("EU") joint review delegation, pursuant to Article 13 of 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* ("Agreement"). The Treasury Department response follows each question.

I. REVIEW SCOPE AND PERIOD

Following the first joint review in February 2011, which covered the period of the first six months after the entry into force of the agreement (1 August 2010 until 31 January 2011), the second joint review will cover the ensuing period from 1 February 2011 until 30 September 2012.

Pursuant to Article 13(1), the joint review should cover "*the safeguards, controls, and reciprocity provisions set out*" in the Agreement. In this context, Article 13(2) specifies that the joint review should have particular regard to:

a) the number of financial payment messages accessed;

b) the number of occasions on which leads have been shared with Member States, third countries, and Europol and Eurojust;

c) the implementation and effectiveness of the Agreement, including the suitability of the mechanism for the transfer of information;

d) cases in which information has been used for the prevention, investigation, detection, or prosecution of terrorism or its financing;

e) compliance with the data protection obligations specified in the Agreement.

Article 13(2) further states that "*the review shall include a representative and random sample of searches in order to verify compliance with the safeguards and controls set out in this Agreement, as well as a proportionality assessment of the Provided Data, based on the value of such data for the investigation, prevention, detection, or prosecution of terrorism or its financing.*"

In order to prepare the second joint review, it would therefore be useful if the following questions could be answered in advance by the US authorities:

II. STATISTICAL INFORMATION

1. In comparison to the period covered by the first joint review, what is the trend of the total number of financial payment messages provided (substantially/slightly higher/lower, about the same)?

The trend of the number of financial messages received from the designated provider has been slightly lower over the course of the 20 months between February 1, 2011, and September 30, 2012 ("the review period"). The decrease may be the result of the Treasury Department's decisions, as part of its ongoing utility-based reviews of the data, to narrow the message types responsive to its Requests on three separate occasions during the review period – in February 2011, September 2011, and October 2011.[7] The decrease also could be the result of a reduction in the international usage of particular message types responsive to the Requests.

2. How many financial payment messages were accessed during the period covered by the review?

During the 20 months of the review period, TFTP analysts conducted 31,797 searches of the TFTP, for an average of 1,590 searches per month. This number includes searches involving data stored in and 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; most will be viewed for a few seconds to determine value and thereafter closed, with no further action or dissemination.

3. In comparison to information provided to EU competent authorities and third-countries, what is the trend of information derived from accessing these payment messages provided to competent US authorities (substantially/slightly higher/lower, about the same)?

The trend of TFTP information provided to EU and third-country authorities has increased substantially during the review period. Please see responses to Questions 4, 5, 10, and 11, below. The Treasury Department has seen a corresponding increase in the TFTP-derived information provided to competent U.S. authorities.

[7] The Treasury Department narrowed the responsive message types an additional time immediately after the review period, in October 2012.

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

During the 20 months of the current review period, U.S. investigators supplied 267 TFTP-derived "reports" pursuant to Article 9 and an additional 606 "leads" pursuant to Article 10 to competent authorities of EU Member States and Europol. A single TFTP report may contain multiple TFTP leads. For example, a single Article 9 spontaneous report provided to Europol during the review period contained 34 TFTP leads.

"Reports" have been used to share TFTP-derived information with EU Member States and third-country authorities – beginning long before the TFTP Agreement in 2010. This mechanism generally involves situations in which U.S. counter-terrorism authorities are working with a counterpart foreign agency on a counter-terrorism case of mutual concern or where U.S. counter-terrorism authorities discover counter-terrorism information that they believe affects or would assist the work of a foreign counterpart. In such situations, TFTP-derived information regarding a particular terrorism suspect or case would be supplied to the foreign counterpart – generally with no indication that any of the information comes from the TFTP. Since the Agreement entered into force in August 2010, the U.S. Government has continued to use reports as the vehicle for the spontaneous provision of information to the competent authorities of EU Member States and Europol pursuant to Article 9. Article 9 reports provided to Europol are explicitly identified as containing TFTP-derived information.

A TFTP "lead", on the other hand, refers to the summary of a particular financial transaction identified in response to a TFTP search that is relevant to a counter-terrorism investigation. Since the start of the current review period, responses to EU Member States and Europol pursuant to their requests under Article 10 have been provided in lead form and are explicitly identified as TFTP-derived information.

More than 2,000 TFTP reports have been provided to the EU in the 11 years since the program began. In addition to these reports, 606 TFTP leads have been provided to EU Member States and Europol during the 20 months of the current review period.

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

U.S. investigators supplied 202 reports resulting from TFTP data to competent authorities of third countries during the 20 months of the current review period (or an average of 10.1 reports per month), as opposed to 31 reports during the six-month first review period (or an average of 5.2 reports per month). This amounts, approximately, to a 94 percent increase in the average number of reports per month provided to third-country authorities. As described in response to Questions 2 and 4, above, these reports generally summarize the results of an investigation of a subject, which will typically encompass multiple TFTP searches, each potentially including numerous messages and may contain multiple leads. More than 3,000 such reports have been provided to competent authorities throughout the world since the program began, the overwhelming majority of which (more than 2,000 such reports, plus an additional 606 leads) have been provided to the EU.

6. **In how many cases was prior consent of competent authorities in one of the EU Member States requested for the transmission of extracted information to third countries, in accordance with Article 7(d) of the Agreement?**

Article 7(d) authorizes the sharing of certain information involving EU persons "subject to the prior consent of competent authorities of the concerned Member State or pursuant to existing protocols on such information sharing between the U.S. Treasury Department and that Member State ....". Since the last joint review, all TFTP-derived information provided to third countries was provided pursuant to existing protocols on information sharing between the U.S. and the relevant Member State. In the event information could not be shared pursuant to existing protocols, the Treasury Department would not disseminate the information without prior consent of the concerned Member States except where the sharing of the data is essential for the prevention of an immediate and serious threat to public security. Because the Treasury Department relied on existing protocols with relevant EU Member States for all information sharing with third countries during the review period, it did not need to rely on this exception for the prevention of an immediate and serious threat to public security to share information.

7. **For the sharing of information with third countries or other appropriate international bodies, what was the remit of their respective mandates as mentioned in Article 7(b) of the Agreement?**

In accordance with Article 7(b), TFTP-derived information was shared only with law enforcement, public security, or counter-terrorism authorities, for lead purposes only, and solely for the investigation, detection, prevention, or prosecution of terrorism or its financing. Certain classified information also was shared with the U.S.-EU Joint Review of the TFTP Agreement in February 2011. Other sensitive and non-public TFTP-derived information was shown to officials from certain EU institutions, such as European Commission officials and Members of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE").

8. **Please elaborate on cases in which the information provided has been used for the prevention, investigation, detection, or prosecution of terrorism or its financing as mentioned in Article 13(2)(d) of the Agreement?**

Please see attached paper.

9. **Did any of these cases end in any judicial findings? If so, did the judicial authority assess the findings received via the extracted information, i.e. was the information accepted as proof of a case or was the proof challenged?**

Article 7(c) provides that TFTP information may be used for lead purposes only and for the exclusive purpose of the investigation, detection, prevention, or prosecution of terrorism or its financing, and such information is shared based on those conditions, meaning that U.S., EU, and third-country authorities may not directly use TFTP information in a judicial proceeding. Instead, the authorities must use the TFTP information as a means to gather the evidence that may properly be presented to a judicial authority.

10. **In how many cases was information provided spontaneously, in accordance with Article 9 of the Agreement? What has been the US Treasury's experience with**

receiving follow-on information conveyed back by Member States, Europol or Eurojust?

During the 20 months of the review period, 267 reports – many containing multiple or even dozens of TFTP leads – were provided to EU Member States and Europol as the spontaneous provision of information pursuant to Article 9 (or an average of 13.4 reports per month), as opposed to 70 reports during the six-month first review period (or an average of 11.7 reports per month). This amounts, approximately, to a 15 percent increase in the average number of Article 9 reports per month provided to competent authorities of EU Member States and Europol.

The Treasury Department rarely, if ever, receives "follow-on information" in response to its spontaneous provision of information pursuant to Article 9 or in response to its provision of information in response to an EU request pursuant to Article 10. The Treasury Department believes that the provision of such follow-on information would greatly enhance its ability to provide meaningful information to EU authorities pursuant to Articles 9 and 10 and encourages the EU, Europol, Eurojust, and EU Member States to establish a procedure to request such information from their authorities and provide it, where possible, to the Treasury Department.

11. 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 94 requests from EU Member States and Europol pursuant to Article 10 during the review period and responded to all 94 requests. TFTP searches resulted in the transmission of leads to the EU in response to 57 of the 94 requests. There were 606 leads contained in the 57 Article 10 responses provided to EU Member States and Europol during the review period. In at least one case, the Treasury Department supplied additional spontaneous information beyond that requested by the EU in its Article 10 request.

III. IMPLEMENTATION AND EFFECTIVENESS OF THE AGREEMENT

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

No.

13. What has been the frequency of requests to Europol and the Designated Provider under Article 4 of the Agreement, and did these requests contain personal data?

During the review period, the Treasury Department submitted its Article 4 Requests on a monthly basis. During one month in 2011, the Treasury Department submitted a second, supplemental request in response to a terrorist attack in Europe.

The initial Treasury Department Requests submitted to Europol following the entry into force of the Agreement contained minimal personal data, such as the names and business addresses of the sender and recipient of the Requests and the names of two top Al-Qaida leaders. In

response to comments provided by Europol, the Treasury Department expanded the amount of personal data included in its Article 4 Requests – such as the names of other terrorists, their supporters, and terrorism-related suspects – in order to provide additional information relating to the provisions of Article 4 regarding the necessity of the data and terrorism-related threats and vulnerabilities.

14. What measures 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 an ongoing review of the extracted 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 relevant to counter-terrorism investigations, and the geographic regions where the terrorist threat is particularly high or most relevant or susceptible to relevant terrorist activity.

The audit and analysis occurs in several stages. First, a comprehensive electronic assessment is conducted of the extracted data to determine the message types and geographic regions that are the most and least responsive to TFTP searches. Second, those message types and geographic regions that have been the least responsive are scrutinized to determine their qualitative component – namely, whether the relatively few responses returned nevertheless contained high-quality information or were of particular value for the purposes of the prevention, investigation, detection, or prosecution of terrorism or its financing. Third, those message types and/or geographic regions that, from a quantitative or qualitative standpoint at the time of the evaluation, do not appear necessary to combat terrorism or its financing are removed from the Article 4 Request.

The Treasury Department refined and narrowed the message types included in its Requests three times during the review period: on two of these occasions (February 2011 and October 2011), the refinement and narrowing were based on the results of the Treasury Department's comprehensive annual audits and analyses and, on the third occasion (September 2011), the refinement and narrowing were based on a determination by the Treasury Department that particular message type(s) were unnecessary for the prevention, investigation, detection, or prosecution of terrorism or terrorist financing based on then-current threat assessments.[8] The Treasury Department also slightly modified the geographic regions responsive to its Requests four times during the review period as a result of evolving threat data (twice expanding the geographic regions responsive to the Request, and twice narrowing them). The Treasury Department will continue to conduct additional necessity-based reviews to ensure that the Requests remain tailored as narrowly as possible.

15. 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?

Article 4 assigns Europol the task to verify whether the Treasury Department Requests:

[8] The Treasury Department narrowed the message types once more immediately after the review period (in its October 2012 Request), based upon completion of its most recent annual audit and analysis.

(a) identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorism financing;

(b) clearly substantiate the necessity of the data;

(c) [are] tailored as narrowly as possible in order to minimize 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

(d) [do] not seek any data relating to the Single Euro Payments Area.

Europol 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". During the review period, Europol performed its verification function, on average, within two days of its receipt of a Treasury Department Request and supplemental documents or its receipt of a Treasury Department response to a Europol request for additional information.

16. 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 never determined that a Treasury Department Request failed to satisfy the requirements set out in Article 4(2). Throughout the review period, Europol regularly provided comments on and requested that the Treasury Department include additional information in the Requests. In addition, the Treasury Department met on repeated occasions with Europol officials, including its data privacy officials, and received from them specific suggestions on how the Requests could be enhanced.

On three occasions during the review period, Europol formally and in writing requested supplemental information with respect to pending Requests. On each occasion, the Treasury Department submitted responsive written supplemental information and Europol verified the pending request. During the summer of 2011, the Treasury Department and Europol agreed that Europol would notify the Treasury Department in advance, if possible, whenever Europol decided that additional types or categories of information could be useful in the Requests, to allow the Treasury Department adequate time to enhance future Requests and to ensure that verification of specific Requests would not be delayed.

17. 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)?

Please see response to Question 16, above.

18. Have any particular issues related to the implementation and effectiveness of the Agreement been identified, including the suitability of the mechanism for the transfer of information? 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.

19. 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.

20. What is the role of U.S. Congress within the oversight mechanism of the TFTP?

The U.S. Congress exercises oversight of the TFTP primarily through the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. The Committees can and do request information on the Treasury Department's counter-terrorism functions, such as the TFTP, and Treasury Department officials periodically brief the Committee on these issues.

IV. COMPLIANCE WITH THE DATA PROTECTION OBLIGATIONS SPECIFIED IN THE AGREEMENT

21. What is the role and what are the findings of the Privacy Officer of the U.S. Treasury Department (Articles 15(3) and 16(2)) in relation to the Agreement? Does this role include findings relevant for the compliance with data protection obligations specified in the agreement (Article 13(2)(e) of the Agreement)?

The Treasury Department's Director for Privacy and Civil Liberties ("Privacy Officer") is the lead Treasury Department official charged with the implementation of Articles 15 and 16 of the Agreement. Under the supervision of the Deputy Assistant Secretary for Privacy, Transparency, and Records and in close coordination with Treasury's Office of General Counsel and Office of Foreign Assets Control ("OFAC"), the Privacy Officer established redress procedures to facilitate the proper implementation of Articles 15 and 16. These redress procedures – allowing persons to seek access, rectification, erasure, or blocking pursuant to Articles 15 and 16 of the Agreement – are posted on the Treasury Department's website at www.treasury.gov/tftp.

The initial step in the redress procedures requires that a person, through the relevant EU National Data Protection Authority ("NDPA"), submit a request in writing pursuant to Articles 15 and/or 16 and provide proof of identity in order to ensure that there are no unauthorized disclosures of personal data. Once a completed request is obtained and identity verified, the Privacy Officer will process the requests as follows: (1) confirm receipt of the completed request (or ask for additional information, where necessary); (2) work with the TFTP manager and/or analysts to verify whether any data relevant to the request have ever been extracted as a result of a TFTP search; (3) assess whether the relevant safeguards with respect to any extraction of data have been satisfied; and (4) provide written notice explaining whether the data subject's rights have been duly respected and, where appropriate, whether personal data may be disclosed (and, if not, the underlying reasons); whether personal data have been rectified, erased, or blocked (and, if not, the underlying reasons); and the means available for seeking administrative and judicial redress in the United States.

The Privacy Officer's role relates to the data protection obligations specified in Articles 15 and 16 of the Agreement. Other officials – including Europol and the independent overseers – have oversight with respect to other data protection obligations specified in the Agreement. Treasury's senior management and counsel,[9] along with the Inspector General of the Treasury Department, have oversight with respect to the entirety of the program.

22. Have any particular issues related to the role or findings of the Privacy Officer of the U.S. Treasury Department been identified (Articles 15(3) and 16(2))?

During the review period, European authorities, including Commission officials and EU NDPAs, raised with the Treasury Department whether the verification of identity of European persons – required by Articles 15 and 16 and the TFTP redress procedures posted on the Treasury Department's website – could be delegated to EU NDPAs. Such a delegation would avoid additional personal data being sent to the United States and authorize those officials closest to requesters – e.g., an NDPA within a requester's own country and presumably familiar with its national identity documents – to make the identity verification decisions that are necessary to ensure the identity of requesters and avoid unauthorized disclosures of personal data.

Treasury Department officials have been working constructively with the Commission to establish uniform NDPA verification procedures, and the Commission has been in communication with the EU's Article 29 Working Party on this topic. Treasury Department officials have provided comments on EU-supplied documents that could be utilized by NDPAs for verification decisions. When documents and procedures are finalized by the Treasury Department and the Commission, the Treasury Department will begin to accept Articles 15 and/or 16 verification decisions by EU NDPAs. The Treasury Department reserves the right to discontinue these special verification procedures if it believes that they are not working satisfactorily.

23. Have any measures put in place to ensure that provided data shall be used exclusively for the prevention, investigation, detection, or prosecution of terrorism and its financing changed since the last Joint Review (Article 5(2))? If so, what changes have occurred?

The most significant change to the Article 5 safeguards has been the Commission's appointment of a deputy overseer, with the agreement of and subject to appropriate security clearances by the United States, in addition to the Commission-appointed overseer appointed pursuant to Article 12. The deputy overseer can share the workload of the overseer and ensure that the overseer work can proceed smoothly while one overseer may be travelling or

[9] The Treasury Department's Office of General Counsel and the Office of the Chief Counsel (Foreign Assets Control) work closely with OFAC, the TFTP manager, and other Treasury officials to review TFTP-related policies and procedures and ensure they are consistent with U.S. obligations under the Agreement, as well as relevant U.S. laws. Counsel support includes, but is not limited to: review of the Request to the Designated Provider and associated supplemental documents provided to Europol to ensure they meet the standards of Article 4; responses to questions regarding the legal sufficiency of a search justification and its associated query to ensure that they satisfy the standards of Article 5; legal guidance regarding the retention and deletion requirements of Article 6, including the necessity-based review; and review of dissemination requests to ensure they comply with the standards of Article 7.

otherwise unavailable. The deputy overseer started work at the Treasury Department on October 1, 2012.

Other than this change, the comprehensive and overlapping set of systems and controls previously reviewed remain in place 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 fulfilment of all requirements for searches, including that a pre-existing nexus to terrorism or its financing is documented for every search; if an analyst even attempted a search that does not satisfy the requirements, the Treasury Department would respond 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 or its financing;

- 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 purpose limitation 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.

24. Have any measures 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 changed since the last Joint Review (Article 5(3))? If so, what changes have occurred?

The enhanced systems and controls outlined in response to Question 23, above, prevent any type of data mining or profiling because they require individualized searches, based on a pre-existing nexus to terrorism or its financing.

25. Have any measures been put in place to implement the provisions of Article 5(4) on data security and integrity or have any measures been changed since the last Joint Review? If so, what changes have occurred?

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 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 unauthorized 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. These measures have been in place for years, and none have changed since the last joint review.

26. Have any measures (other than the measures mentioned in Article 12) 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 (Article 5(5)), or have any such measures been changed since the last Joint Review? If so, what changes have occurred?

Please see response to Question 23, above.

27. Have there been any cases where the extracted data included personal data revealing racial or ethnic origin, political opinions, or religious or other beliefs, trade union membership, or health and sexual life (sensitive data)? If so, have any special safeguards or measures been taken to take into account the sensitivity of these data (Article 5(7))?

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

28. Have any measures put in place to organise the on-going and at least annual evaluation to identify non-extracted data that are no longer necessary to combat terrorism or its financing changed since the last Joint Review (Article 6(1)? If so, what changes have occurred? Have such data been promptly and permanently deleted since the last Joint Review?

Please see response to Question 14, above. Once a message type or geographic region is deleted from the Request, all previous non-extracted data that had been received involving that message type or geographic region are permanently deleted during the course of an annual deletion process. This deletion has occurred with respect to all data received in response to message types or geographic regions removed from the Request during the review period.

29. Have there been any cases where financial payment messaging data were transmitted which were not requested? If so, has the U.S. Treasury Department promptly and permanently deleted such data and informed the relevant Designated Provider (Article 6(2))?

No.

30. Have all non-extracted data received prior to 20 July 2007 been deleted as provided for in Article 6(3) of the Agreement?

Yes. All such data were deleted prior to July 20, 2012, in accordance with Article 6(3).

31. Have any measures taken to provide for the on-going and at least annual evaluation to continuously assess the data retention periods specified in Article 6(3) and 6(4) of the Agreement changed since the last Joint Review? If so, what changes have occurred?

The Treasury Department continues to assess these data retention periods as part of its regular review, analysis, and audit of data, as described in response to Question 14, 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.

32. How is it ensured that the time period for deletion of the data five years after their reception referred to in Article 6(4) of the Agreement is met in reality? Are automatic deletions of non-extracted data foreseen to this end?

Treasury conducts an exhaustive annual evaluation to ensure that any non-extracted data received on or after July 20, 2007, are deleted five years from receipt. This process is technologically intensive, requiring significant time and labor to complete while ensuring that the system remains fully operational and all safeguards remain in place. Based on previous deletions of TFTP data, Treasury has determined that any deletion effort conducted more frequently than on an annual basis could significantly impair the functioning of the system and be technologically infeasible. Treasury also has assessed that automatic deletions of non-extracted data without a thorough evaluation of the data identified for deletion could result in the inadvertent deletion of extracted data necessary for specific on-going counter-terrorism investigations and would not allow for the necessary controls and independent assessments to ensure that the appropriate data had been deleted.

33. Have there been any cases where these retention periods have been reduced in by the U.S. Treasury Department accordance with Article 6(5)?

Please see response to Questions 28 and 31, above.

34. Have any measures 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 changed since the last Joint Review? If so, what changes have occurred?

No changes have occurred since the last joint review. The Treasury Department continues to notify 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.

35. Have any measures 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 changed since the last Joint Review? If so, what changes have occurred?

No changes have occurred since the last joint review. TFTP-derived information continues to be shared with counter-terrorism, law enforcement, or public security authorities in the United States, EU Member States, third countries, and 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 approval by management trained on the safeguards identified in the Agreement. Any subsequent dissemination requires the express written 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.

36. In how many cases have the overseers mentioned in Article 12(1) of the Agreement blocked any searches on the grounds that they appear to be in breach of Article 5 of the Agreement? Can any typical kind of be identified where blocking was deemed necessary? If so, please elaborate. How many searches have been blocked by the EU appointed overseer(s) or the overseer(s) appointed by the Designated Provider(s) on the grounds indicated above? If possible, please make a distinction between temporary and permanent blocking of searches and the origin of the overseer.

The overseers mentioned in Article 12 of the Agreement – two 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 the

overwhelming majority of cases, the overseers request additional information simply for routine auditing purposes and not out of any concern with the search itself.

During the review period, the overseers queried 791 searches – virtually all of which were selected for routine auditing purposes. All searches queried by the overseers are blocked until the overseers' concerns have been fully addressed. In the overwhelming majority of all searches conducted (well over 99.9 percent), the overseers were fully satisfied with the search as formulated. In a small number of cases (57 searches during the 20 months of the review period – or .0018 percent), the overseers blocked the searches because they believed the search terms were too broad. In all 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 satisfied the overseers. In cases where the searches were identified through retrospective review, no information obtained through the searches was disseminated or used unless and until the overseers were satisfied.

In terms of the 791 searches queried, the Treasury Department cannot accurately break them down between the Designated Provider and the EU overseer, because when one party queried a search, it was treated as queried by the overseers generally.

37. Have any measures taken to ensure that the results of the searches are not disseminated before the overseers have had a chance to review the search changed since the last Joint Review? If so, what changes have occurred?

No changes have occurred since the last joint review. Any dissemination of TFTP-derived information continues to require management approval, and subsequent dissemination requires the express approval of the Treasury Department. The Treasury Department trains counter-terrorism analysts on the proper procedures for using, and/or requesting and receiving approval to disseminate 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, and no information obtained through TFTP searches was disseminated over the objections of the overseers.

38. Have there been any cases where individuals have exercised their rights of 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?

During the review period, the Treasury Department received five cases in which individuals apparently sought to exercise the right of access described in Article 15 of the Agreement. Because these requests did not conform to the TFTP redress procedures posted on the Treasury Department's public website (www.treasury.gov/tftp), the Treasury Department responded in all five cases by requesting certain additional basic information, pursuant to the Treasury Department procedures, including that the requests be signed by the requesters and contain confirmation that the requesters consent to any personal data being shared with the NDPAs. Neither the NDPAs nor the requesters responded to the Treasury Department with the additional requested information.

Two other individuals sent emails to the TFTP email address posted on the Treasury Department's TFTP web page (www.treasury.gov/tftp) 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 individuals to EU and Treasury Department websites containing additional information on how to submit requests. Neither the individuals nor the relevant NDPA submitted an Article 15 or 16 request. The Treasury Department also received emails from an EU NDPA inquiring about possible cost to the requester for an Article 15 or 16 request, and the Treasury Department responded.

39. 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, including but not limited to supplementation, deletion or correction (Article 17(1))?

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

40. Were any notifications regarding inaccuracy or unreliability of transmitted information made by either of the Parties as set out in Article 17(2) of the Agreement? If so, please elaborate.

No.

41. Were any notifications and consultations regarding redress made by either of the Parties as set out in Article 18(1) of the Agreement? If so, please elaborate.

No.

42. Have there been any cases where individuals have made use of the means of redress provided for under 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 38, above.

If possible and where relevant, please make available documentation related to the measures and procedures put in place for the various safeguards under the agreement, especially those mentioned in Articles 4, 5, 6, 7, 12, 15 and 16.

ANNEX III[10]

EUROPOL STATISTICAL INFORMATION REGARDING ARTICLES 4, 9 AND 10 OF THE AGREEMENT

A. Summary of statistics for Article 4 requests under the TFTP Agreement:

Period	**01 August 2010 – 27 September 2012**				
Month	Article 4 request		Request for supplemental information and reply		
	Date of receipt	Number of pages	Yes/No	Date of request	Date of reply
Aug-10	06/08/2010	51	Yes	06/08/2010	09/08/2010
Sep-10	08/09/2010	51	No	-/-	-/-
Oct-10	05/10/2010	53	Yes	06/10/2010	08/10/2010
Nov-10	02/11/2010	55	Yes	03/11/2010	03/11/2010
Dec-10	22/12/2010	58	No	-/-	-/-
Jan-11	07/01/2011	58	No	-/-	-/-
Feb-11	14/02/2011	58	Yes	15/02/2011	17/02/2011
Mar-11	09/03/2011	63	Yes	09/03/2011	22/03/2011
Apr-11	07/04/2011	66	No	-/-	-/-
May-11	04/05/2011	69	No	-/-	-/-
Jun-11	09/06/2011	69	Yes	10/06/2011	17/06/2011
Jul-11 (1)	15/07/2011	77	No	-/-	-/-
Jul-11 (2)	26/07/2011	12	No	-/-	-/-
Aug-11	02/08/2011	79	No	-/-	-/-
Sep-11	08/09/2011	80	No	-/-	-/-
Oct-11	14/10/2011	82	No	-/-	-/-
Nov-11	16/11/2011	81	No	-/-	-/-
Dec-11	12/12/2011	81	No	-/-	-/-
Jan-12	09/01/2012	82	No	-/-	-/-
Feb-12	10/02/2012	83	No	-/-	-/-
Mar-12	08/03/2012	81	No	-/-	-/-
Apr-12	11/04/2012	83	No	-/-	-/-
May-12	10/05/2012	94	No	-/-	-/-
Jun-12	06/06/2012	96	No	-/-	-/-
Jul-12	12/07/2012	99	No	-/-	-/-
Aug-12	08/08/2012	100	No	-/-	-/-
Sep-12	12/09/2012	104	No	-/-	-/-
		73 Average (rounded)			

[10] It is important to note that this annex (and the statistical information provided therein) covers the whole period since the entry into force of the agreement on 1.8.2010.

B. Overview regarding verification communication and total set of documentation:

Period	01 August 2010 – 27 September 2012		
Month	Communication with the Designated Provider		Total set of verification documentation (including DPO advice, verification decision)
	Delay notification[11]	Verification	Number of pages
Aug-10	06/08/2010	10/08/2010	66
Sep-10	10/09/2010	14/09/2010	61
Oct-10	07/10/2010	08/10/2010	65
Nov-10	-/-	04/11/2010	61
Dec-10	-/-	23/12/2010	64
Jan-11	07/01/2011	10/01/2011	64
Feb-11	16/02/2011	17/02/2011	74
Mar-11	11/03/2011	25/03/2011	86
Apr-11	-/-	08/04/2011	78
Ma-11	-/-	05/05/2011	79
Jun-11	09/06/2011	17/06/2011	83
Jul-11 (1)	15/07/2011	19/07/2011	86
Jul-11 (2)	-/-	27/07/2011	17
Month	Communication with the Designated Provider		Total set of verification documentation (including DPO advice, verification decision)
	Delay notification	Verification	Number of pages
Aug-11	-/-	02/08/2011	84
Sep-11	09/09/2011	12/09/2011	87
Oct-11	14/10/2011	18/10/2011	89
Nov-11	-	17/11/2011	89
Dec-11	-	12/12/2011	89
Jan-12	-	10/01/2012	90
Feb-12	13/02/2012	17/02/2012	92
Mar-12	09/03/2012	16/03/2012	92
Apr-12	-	13/04/2012	91
May-12	-	11/05/2012	103
Jun-12	-	08/06/2012	104
Jul-12	-	13/07/2012	108
Aug-12	-	10/08/2012	110
Sep-12	-	13/09/2012	112
			82 Average (rounded)

[11] A notification of delay is issued by Europol to the concerned parties when the verification process is expected to take longer than 48 hours of working days.

C. Summary of monthly figures (as per 27 September 2012)

2010:

Month	08 2010	09 2010	10 2010	11 2010	12 2010
Article 4	1	1	1	1	1
Article 9[12]	6	1	1	0	0
Article 10[13]	0	1	0	0	1

2011:

Month	01 2011	02 2011	03 2011	04 2011	05 2011	06 2011	07 2011	08 2011	09 2011	10 2011	11 2011	12 2011
Article 4	1	1	1	1	1	1	2	1	1	1	1	1
Article 9	1	0	0	0	1	7	0	0	0	0	0	0
Article 10	4	4	10	6	5	8	12	7	4	9	3	3

2012:

Month	01 2012	02 2012	03 2012	04 2012	05 2012	06 2012	07 2012	08 2012	09 2012
Article 4	1	1	1	1	1	1	1	1	1
Article 9	0	0	0	0	0	0	1	0	0
Article 10	4	6	2	1	3	7	4	6	0

Overall:

08/2010 – 09/2012	Sum
Article 4	27
Article 9	18
Article 10	110

Breakdown Article 10 requests	
EU Member States	94
Europol	14
Eurojust	2

D. Summary of intelligence leads (as per 27 September 2012)

Article 9: Information spontaneously provided by the US	
Instances	**Leads**
18	88
Article 10: Requests and generated leads	
110	456

[12] The figures refer to the number of instances of information provided by the US authorities under Article 9, routed through Europol; the number of intelligence leads is shown in the graph under Section D below (bilateral information to EU MS is not included).

[13] The figures refer to the number of instance of information requests under the Article 10, routed through Europol; the number of intelligence leads is shown in the graph under Section D below (bilateral information requests between EU MS and US are not included).

ANNEX IV

RECENT EXAMPLES OF CASES IN WHICH TFTP INFORMATION HAS BEEN USED FOR THE PREVENTION, INVESTIGATYION, DETECTION OR PROSECUTION OF TERRORISM OR ITS FINANCING

(AS OF OCTOBER 2012)

Treasury's Terrorist Finance Tracking Program (TFTP) is a vital counter-terrorism tool that in its 11-year history has produced thousands of TFTP-derived leads to counter-terrorism authorities, including more than 2,000 TFTP reports (which may contain multiple TFTP leads) provided to European authorities and over 3,000 such reports shared globally. In addition to these reports, 606 TFTP leads have been provided to EU Member States and Europol during the period from 1 February 2011 through 30 September 2012. TFTP data provides key information including account numbers, names, addresses, transaction amounts, dates, branch locations, and sometimes even bills of lading that are of tremendous value for counter-terrorism analysts in identifying previously unknown terrorist operatives and financial supporters. The examples below highlight cases in which TFTP has provided key leads, as well as the ways in which TFTP-derived data have helped to identify the financial support networks behind leading terrorist organizations currently under investigation by U.S. and European authorities. The following are examples associated with five of the most concerning groups and are by no means an exhaustive list of groups for which TFTP has been used.

Al-Qaida

Background/Context:

Established by Usama Bin Ladin in 1988, and responsible for the September 11, 2001 attacks, Al-Qaida and Al-Qaida-affiliated groups have since 2002 conducted attacks worldwide, including in Europe, North Africa, South Asia, Southeast Asia, and the Middle East. On May 2, 2011, U.S. forces raided a compound in Abbottabad, Pakistan, resulting in the death of Bin Ladin. Despite Bin Ladin's death and other significant leadership losses, Al-Qaida remains a cohesive organization and has advanced several unsuccessful Western plots in the past two years, including against the United States and Europe.

Since the attacks of September 11, 2001, the TFTP has been used to identify and investigate individuals and organizations suspected of providing financial support to Al-Qaida. These investigations have resulted in thousands of TFTP-derived leads identifying the names, locations, phone numbers, and accounts of previously unknown Al-Qaida operatives and supporters. Much of this information has been passed to counter-terrorism authorities around the world to further their investigations.

Recent TFTP Case Examples:

TFTP-derived information was used in the investigation of Al-Qaida facilitator Adel Radi al-Harbi, contributing to his eventual designation in October 2012 by the Treasury Department as a specially designated global terrorist (SDGT) pursuant to Executive Order 13224, which blocks the property and prohibits transactions with persons who commit, threaten to commit, or support terrorism. Al-Harbi is the deputy commander of Al-Qaida's Iran-based facilitation network. He continues to facilitate travel for extremists, raise funds for attacks, as well as provide technical support for Al-Qaida's internet presence. Under the State Department's Rewards for Justice Program, the U.S. Government is offering 5 million U.S. dollars for information leading to the location of al-Harbi. He is also on the Saudi Arabian Ministry of Interior's Most Wanted List.

TFTP-derived information was used in the investigation of Al-Qaida operative Abd al-Raham Ould Muhammad al-Husayn Ould Muhammad Salim, contributing to his eventual designation in September 2011 as a SDGT by the Treasury Department under Executive Order 13224. Salim was arrested in Pakistan in September 2011. Salim helped form the merger between Al-Qaida and Al-Qaida in the Islamic Maghreb (AQIM) and served as Al-Qaida's external operations chief until his arrest. In early 2010, Usama Bin Ladin personally dedicated a large sum of money to Salim to develop a plan to destroy Europe's economy. In mid-2010, Salim was recruiting operatives for a European plot.

Also, TFTP-derived information was used in the investigation of a European Union citizen and Al-Qaida recruiter, who lived most of his adult life in Germany until his recent arrest in Pakistan. He was a known associate of European extremists and was identified as the recruiter for a foiled European plot that involved gun seizures in major European cities.

Al-Qaida in the Lands of the Islamic Maghreb (AQIM)

Background/Context:

AQIM is an Algeria-based terrorist group. AQIM operates primarily in northern coastal areas of Algeria and in parts of the desert regions of southern Algeria and northern Mali. Its principal sources of funding include extortion, kidnapping, donations, and narcotics trafficking. AQIM officially joined Al-Qaida in September 2006. AQIM subsequently expanded its aims from overthrow of the Algerian government to attacking Western targets, and executed several conventional terrorist attacks against such targets between late 2006 and early 2008. The group added the use of suicide bombings in April 2007, with attacks against government ministry and police buildings in Algiers that killed more than 30 people. AQIM leader Abdelmalek Droukdal announced in May 2007 that suicide bombings were going to become the group's main tactic. The group claimed responsibility for a suicide truck bomb attack that killed at least eight soldiers in Algeria on July 11, 2007, the opening day of the All-Africa Games. AQIM continues to target Westerners and has successfully kidnapped

numerous Westerners for ransom, a tactic that predates its merger with Al-Qaida. In May 2009, AQIM announced it killed a British hostage after months of failed negotiations. In June of the same year, the group publicly claimed responsibility for killing U.S. citizen Christopher Leggett in Mauritania because of his missionary activities. In 2010, multinational counter-terrorism efforts – including a joint French-Mauritanian raid in July against an AQIM camp – resulted in the deaths of some AQIM members and possibly disrupted some AQIM activity. In 2011, however, AQIM killed two French hostages during an attempted rescue operation. AQIM continues to hold four French hostages, demanding at least 90 million euros for their release. AQIM also is still holding an Italian tourist kidnapped in Algeria.

The TFTP has been used to identify and investigate individuals and organizations suspected of providing financial and other support to AQIM.

Recent TFTP Case Examples:

TFTP-derived information was used in the investigation of Nabil Abu Olkoma, deputy commander of AQIM's Tareq ibn Ziyad Brigade. Olkoma was killed in a car crash in September 2012.

TFTP-derived information was used in the investigation of an AQIM senior leader. The AQIM leader was recently arrested in Algeria while travelling to meet with other AQIM sections. When caught, he had weapons, ammunition, and other documents.

TFTP-derived information was used in the investigation of Kamil Bouihane, AQIM communications chief. Bouihane was killed in a raid in Algeria in February 2011. He was involved in planning suicide bombings in Algeria, including the 2007 bombing of a UN office in Algiers.

Al-Qaida in the Arabian Peninsula (AQAP)

Background/Context:

Yemen-based AQAP emerged in January 2009 following an announcement that Yemeni and Saudi terrorists were unifying under a common banner, signaling the group's intent to serve as a hub for regional terrorism in Yemen and Saudi Arabia. AQAP is based primarily in the tribal areas outside of Sanaa, which for the most part remain largely outside the control of the Yemeni Government. The group has targeted local, U.S., and Western interests in the Arabian Peninsula, but is now pursuing a global strategy. AQAP's predecessor, Al-Qaida in Yemen (AQY) was founded in February 2006 by 23 Al-Qaida members who had escaped from Yemeni prison. In September 2006, AQY operatives conducted near-simultaneous suicide attacks against Yemeni oil facilities, and, in early 2008, AQY carried out small-arms attacks on foreign tourists and a series of mortar attacks against the U.S. and Italian Embassies in Sanaa, the Presidential Compound, and Yemeni military complexes. In September 2008, the group targeted the U.S. Embassy in Sanaa using two vehicle bombs, killing 19 people, including six terrorists. Since unifying as AQAP in 2009, the group has orchestrated high-

profile terrorist attacks and expanded its activities outside of Yemen, most notably including the attack by Nigerian-born Umar Farouk Abdulmutallab, who attempted to detonate an explosive device aboard a Northwest Airlines flight on December 25, 2009 – the first attack inside the United States by an Al-Qaida affiliate since September 11, 2001. That was followed by an attempted attack in which explosive-laden packages were sent to the United States on October 27, 2010. Most recently, AQAP was responsible for the foiled bomb plot that was timed for the anniversary of Usama Bin Ladin's death, May 2, 2012. In this plot, a suicide bomber wearing a more sophisticated version of Abdulmutallab's 2009 bomb was targeting an airliner bound for the United States.

The TFTP has been used to identify and investigate individuals and organizations suspected of providing financial and other support to AQAP.

Recent TFTP Case Examples:

TFTP-derived information was used in the investigation of suspected AQAP facilitators. Research revealed a bank account in the Middle East belonging to a possible AQAP associate. The resulting TFTP-derived information helped investigators better map and target AQAP's financial network.

TFTP-derived information was used in the investigation of an AQAP operative who was recently arrested in the UK on a U.S. extradition warrant. The individual was arrested for receiving military training in Yemen, as well as providing material support to AQAP. If convicted on all charges, this individual would face a maximum sentence of life in prison.

TFTP-derived information is continuing to be used in the investigation of an AQAP operative and suspected operations commander. This operative has been involved in raising funds for AQAP operations, as well as stockpiling weapons for future attacks.

Al-Shabaab

Background/Context:

The Harakat Shabaab al-Mujahidin (al-Shabaab) was the militant wing of the Somali Council of Islamic Courts that took over most of southern Somalia in the second half of 2006. Although the Somali government and Ethiopian forces defeated the group in a two-week war between December 2006 and January 2007, al-Shabaab – a clan-based insurgent and terrorist group – has continued its violent insurgency in southern and central Somalia. The group has exerted temporary and, at times, sustained control over strategic locations in southern and central Somalia by recruiting, sometimes forcibly, regional sub-clans and their militias. Al-Shabaab's senior leadership is affiliated with Al-Qaida, and certain extremists aligned with al-Shabaab are believed to have trained and fought in Afghanistan. Al-Shabaab has issued statements praising Usama Bin Ladin and linking Somalia to Al-Qaida's global jihad operations. The group has claimed responsibility for many bombings – including various types of suicide attacks – in Mogadishu and in central and northern Somalia, typically

targeting Somali Government officials and perceived allies. Al-Shabaab also is responsible for the assassination of Somali peace activists, international aid workers, numerous civil society figures, and journalists. The group gained additional notoriety by blocking the delivery of aid from some Western relief agencies during a 2011 famine that has killed tens of thousands and still threatens millions of Somalis. Al‑Shabaab was listed for targeted sanctions in April 2010 by the United Nations Security Council Committee established pursuant to resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea. The Committee listed al-Shabaab for being an entity engaged in acts that directly or indirectly threaten the peace, security, or stability of Somalia. The European Union similarly listed al-Shabaab on September 26, 2011. The U.S. Government has also designated al-Shabaab under its counter-terrorism authorities, including as a SDGT under Executive Order 13224. Al-Shabaab is also listed on the Annex to Executive Order 13536, which targets, among other things, threats to the peace, security, and stability of Somalia.

The TFTP has been used to identify and investigate individuals and organizations suspected of providing financial and other support to al-Shabaab.

Recent TFTP Case Examples:

TFTP-derived information provided information related to al-Shabaab members in Europe. Research revealed the European bank accounts and addresses of three al-Shabaab associates from late-2011 to mid-2012.

TFTP-derived information was used in the investigation of an al-Shabaab operative who was involved in the double suicide attack in Uganda that killed 74 people watching a World Cup match. This individual has been arrested and is awaiting trial.

TFTP-derived information was used in the investigation of al-Shabaab facilitator Abu Faris, who was designated in July 2012 pursuant to Executive Order 13536 for contributing to the conflict in Somalia. In particular, since 2007, Faris has facilitated travel for foreign fighters as well as provided financial assistance for foreign fighters in Somalia.

The Islamic Jihad Union (IJU)

Background/Context:

The IJU is an extremist organization that splintered from the Islamic Movement of Uzbekistan in the early 2000s. The IJU first conducted attacks in April 2004, killing approximately 47 people and marking the first use of suicide bombers in Central Asia. In July 2004, the group struck again, with near-simultaneous suicide bombings of the U.S. and Israeli Embassies and the Uzbekistani Prosecutor General's office in Tashkent. The IJU stated that the attacks were committed in support of IJU's Palestinian, Iraqi, and Afghan brothers in the global insurgency. In September 2007, German authorities detained three IJU operatives, disrupting an IJU plot against unidentified U.S. or Western facilities in Germany. The operatives

acquired roughly 700 kg of hydrogen peroxide and an explosives precursor, which was enough raw material to make the equivalent of approximately 544 kg of TNT. The IJU subsequently claimed responsibility for the foiled plot. The three operatives, along with a fourth man detained several months later in Turkey, were put on trial in Germany in 2009 and convicted. IJU members are scattered throughout Central Asia and parts of South Asia, including Afghanistan, where the group has claimed responsibility for attacks against Coalition forces.

TFTP-derived information continues to help track, identify, and investigate individuals and organizations suspected of providing financial and other support to the IJU.

Recent TFTP Case Examples:

Within the last two years, TFTP-derived information has been used in the investigation of an IJU facilitator and member of the German Taliban Mujahedin.

TFTP-derived information is continuing to be used in the investigation of an IJU facilitator and recruiter. This facilitator was implicated in a European bomb plot and has been sentenced in absentia by a foreign government for conducting terrorist actions.

Within the last two years, TFTP-derived information has been used in the investigation of an IJU operative who was suspected of planning a terrorist attack.

*** * ***