EUROPEAN
COMMISSION

Brussels, 19.1.2017
SWD(2017) 17 final

COMMISSION STAFF WORKING DOCUMENT

Joint Review Report 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

Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

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

{COM(2017) 31 final}

Table of Contents

1. BACKGROUND

The Terrorist Finance Tracking Program (TFTP) was set up by the U.S. Treasury Department shortly after the terrorist attacks of 11 September 2001 when it began issuing legally binding production orders to a provider of financial payment messaging services for financial payment messaging data stored in the United States that would be used exclusively in the fight against terrorism and its financing.

Until the end of 2009, the provider stored all relevant financial messages on two identical servers, located in Europe and the United States. On 1 January 2010, the provider implemented its new messaging architecture, consisting of two processing zones – one zone in the United States and the other in the European Union.

In order to ensure the continuity of the TFTP under these new conditions, a new Agreement between the European Union and the United States on this issue was considered necessary. After an initial version of the Agreement did not receive the consent of the European Parliament, a revised version was negotiated and agreed upon in the summer of 2010. The European Parliament gave its consent to the Agreement on 8 July 2010, the Council approved it on 13 July 2010, and it entered into force on 1 August 2010.

2. PROCEDURAL ASPECTS

Article 13 of the Agreement provides for regular joint reviews of the safeguards, controls, and reciprocity provisions to be conducted by review teams from the European Union and the United States, including the European Commission, the U.S. Treasury Department, and representatives of two data protection authorities from EU Member States, and may also include security and data protection experts and persons with judicial experience.

Pursuant to Article 13 (2) of the Agreement, the 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."

This report concerns the fourth joint review of the Agreement since it entered into force and covers a period of 22 months between 1 March 2014 and 31 December 2015. The first joint review of the Agreement conducted in February 2011[1] covered the period of the first six months after the entry into force of the Agreement (1 August 2010 until 31 January 2011) and the second joint review conducted in October 2012[2] covered the subsequent period of twenty months (1 February 2011 until 30 September 2012). The third joint review conducted in April 2014 covered a period of seventeen months (1 October 2012 until 28 February 2014).[3] On 27 November 2013, the Commission adopted the Communication on the Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement[4].

In line with Article 13 (3), for the purposes of the review, the European Union was represented by the European Commission, and the United States was represented by the U.S. Treasury Department. The EU review team was headed by a senior Commission official and in total consisted of two members of Commission staff, representatives of two data protection authorities, and one judicial expert from Eurojust. A list of the members of both the EU and US review teams is included in Annex I to this Report.

The fourth joint review was carried out in two main steps: on 1 March 2016 in The Hague at Europol's premises and on 15 and 16 March 2016 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 briefed by Europol senior staff and experts on Europol's implementation of the Agreement. The teams visited the secure location where Europol handles the U.S. requests. Prior to the visit, Europol provided a written contribution to the review, including the relevant statistical information (Annex III).

– To prepare the visit in Washington, the EU team had sent a questionnaire to the Treasury in advance of the review. This questionnaire contained a range of 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 posed further questions to Treasury officials and was able to address all the various parameters of the Agreement.

– The EU team had sent the Treasury a selection of a representative and random sample of searches to be verified during the review visit.

– The review team members were granted access to the TFTP facilities in the Treasury. For security reasons, review team members were required to provide advance evidence of their security clearances to access the TFTP facility and to sign a copy of

[1] SEC(2011) 438 final
[2] SWD(2012) 454 final
[3] COM (2014) 513 final and SWD (2014) 264 final of 11.8.2014
[4] COM (2013) 843 final of 27.11.2013

a non-disclosure agreement as a condition for their participation in this review exercise.

– 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 U.S. confidentiality requirements.

– The review teams had direct exchanges with Treasury personnel responsible for the implementation of the TFTP program, the Treasury's Office of the Assistant General Counsel for Enforcement and Intelligence, the Director for Privacy and Civil Liberties and the Deputy Assistant Secretary for Privacy, Transparency and Records, the overseers who review the searches of the data provided under the TFTP Agreement, and the auditor of the TFTP employed by the Designated Provider.

– The review teams were given a demonstration of and explanations about dissemination and scrutiny log files.

This report is based on the 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, during the review, was used and the inspection report of Europol's Joint Supervisory Body (JSB) from September 2015[5] was considered. To complete the information available to it, the Commission also met and received information from the Designated Provider.

Due to the sensitive nature of the TFTP some information was provided to the review team under the condition that it would be treated as classified up to the level of EU SECRET. Certain classified information was only made available for consultation and reading on the Treasury premises. All members of the EU team had to sign non-disclosure agreements exposing them to criminal and/or civil sanctions for breaches. However, this did not hamper the work of the joint review team and all issues identified during the review are included in this report.

As in case of the past reviews, the fourth 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 results of the review in a manner which is as objective as possible.

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. The Commission would like to acknowledge the excellent cooperation on the part of all Treasury and other U.S. personnel, Europol's and the Designated Provider's staff, as well as the two EU overseers.

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

[5] http://www.europoljsb.europa.eu/media/275252/15-28%20final%20tftp%202015%20inspection%20report.pdf

on the EU side. However, the modalities for the fourth review and the procedure for the issuance of this report were agreed with the Treasury, including an opportunity for the latter of prior reading of this report for the purpose of identifying any classified or sensitive information that could not be disclosed to the public.

This report and the recommendations contained herein have been approved by the members of the EU review team.

3. THE OUTCOME OF THE JOINT REVIEW

3.1. The value of the TFTP Provided Data

In line with Article 13 (2) of the Agreement, the proportionality of the TFTP Provided Data should be assessed on the basis of the value of such data for the fight against terrorism and its financing. Understanding the ways in which the TFTP-derived information may be used as well as the provision of concrete examples as underlying evidence is the balanced approach for such an assessment.

Since the entry into force of the Agreement and in response to the Commission's requests, the U.S. authorities have become increasingly transparent in sharing information illustrating the value of the TFTP.

During the first joint review, the Treasury provided several classified examples of high profile terrorism-related cases where TFTP-derived information had been used. For the second joint review, the Treasury provided an annex containing 15 concrete examples of specific investigations in which TFTP provided key leads to counter-terrorism investigators.

Pursuant to Article 6 (6) of the Agreement, the Commission and the Treasury prepared a joint report regarding the value of the TFTP Provided Data (Joint Value Report)[6]. The Joint Value Report of 27 November 2013 explains how the TFTP has been used and includes many specific examples where the TFTP-derived information has been valuable in counter-terrorism investigations in the United States and the EU.

In the course of the third joint review, the Treasury emphasised the importance of the TFTP for global counter-terrorism efforts as a unique instrument to provide timely, accurate and reliable information about activities associated with suspected acts of terrorist planning and financing. The TFTP helps to identify and track terrorists and their support networks.

In addition to the examples provided during the past three reviews and in the Value Report, eighteen recent cases included in Annex IIA further demonstrate how the TFTP helped international counter-terrorism efforts. The review team heard from the Treasury analysts how the TFTP information is analysed and was given classified presentations of recent examples of counter-terrorism cases around the world in which TFTP information played a decisive or important role.

[6] COM(2013) 843 final of 27.11.2013

The Commission welcomes the efforts of the Treasury to collect, analyse and make available to the review team and to the public examples demonstrating the important value of the TFTP despite the limitations given by the nature of highly sensitive counter-terrorism investigations.

On the basis of the information provided by the Treasury, Europol and EU authorities over the time, the Commission is of the view that the TFTP remains an important and efficient instrument contributing to the fight against terrorism and its financing in the United States, the EU and elsewhere.

3.2. 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.

Pursuant to Article 9, the Treasury 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 U.S. if it determines that there is reason to believe that a person or entity has a nexus to terrorism or its financing. There is no legal obligation for the Treasury and Member States to channel Article 9 and 10 TFTP-derived information and requests through Europol. The review team notes that Europol was involved in almost all Member States' requests under Article 10 and in most cases of provision of spontaneous information under Article 9.

The use of this mechanism by Member States and the EU has increased since the initial phase of the implementation of the Agreement. There were fifteen requests from Member States and the EU received by the Treasury under Article 10 during the six-month period covered by the first review report. During the twenty months covered by the second review, Member States and the EU submitted 94 requests to the Treasury. The Treasury received 70 requests during the seventeen months covered by the third review. Under the current review, the Treasury received 192 such requests. Europol has initiated in the current review period 74 requests and transmitted 120 requests from Member States.[7] There were no new requests by Eurojust covered by this review.

The number of leads generated by the TFTP in response to Article 10 requests has increased significantly. During the review period, there were 8,998 leads contained in the 121[8]

[7] The total number of requests sent by Europol during this review period is slightly lower than the total number received by the Treasury during this period, because of differences in when requests are received and registered.

[8] The Treasury responded to all 192 requests received from Member States and the EU during the review period. Of these requests, 69 searches were returned without results. Such responses may provide valuable information to a counter-terrorism investigator, including that the target may not be using the formal financial system to conduct transactions or that the target is no longer conducting transactions using a particular financial service provider. The Treasury notes that, due to the timing of some of the 192 requests, some of the responses were provided to Europol after the conclusion of the review period.

responses provided to Member States and Europol as compared to 3,929 leads contained in the 41 responses provided to Member States and Europol during the period of the third review.

Annex IIA also includes examples of terrorism-related investigations by European authorities. During the review period the TFTP provided leads relating to several terrorist suspects, including foreign fighters travelling to or returning from Syria and the support networks facilitating or funding their movements and training. The TFTP also played an important role in the investigations following the terrorist attacks in Paris of 13 November 2015, where the Treasury provided EU authorities within the period under review with more than 900 TFTP-derived leads (pursuant to Article 9 and 10 of the Agreement).

Throughout the implementation of the Agreement, Europol played an active role in raising the awareness on the possibilities available under the TFTP by promoting the reciprocity provisions through dedicated campaigns in Member States. For instance, Europol has organised several practitioners meetings with the aim of maximising the use of the TFTP, both in the interests of the US authorities and of Member States. In addition, Europol has proactively initiated a series of requests under Article 10 of the Agreement in the period under review. This has helped raise awareness of added value of the TFTP among EU authorities, resulting in an increased use of the TFTP by those authorities.

Pursuant to Article 9, U.S. investigators supplied 93 TFTP-derived reports consisting of 2,680 leads during this review period. This figure includes both the information provided to/through Europol and directly to Member States' authorities. Usually the information provided directly would be shared in the context of an investigation of a counter-terrorism case of mutual concern for the U.S. and a Member State.

The U.S authorities submitted that they received positive feedback from Europol and certain EU Member States on the added value of information provided under the TFTP. However, in general, and in line with what was submitted in the third joint review, the Treasury explained that the U.S. authorities often lack feedback on the usefulness of the TFTP leads supplied to Member States under Articles 9 and 10 of the Agreement. Such information would help to understand Member States' needs better, the desirability of a follow-up of cases and would further improve the future provision of TFTP leads. Europol has informed the review team that it always reminds the Member State receiving information under the Agreement to provide constructive feedback in relation to the accuracy and relevance of the data transmitted. Such feedback appears not to be provided in all cases.

The Commission proposes that Member States consider providing regular feedback on the TFTP data received from the Treasury, which could further improve the quality and the quantity of information exchanged under Articles 9 and 10 of the Agreement. The Commission suggests that Europol continues its efforts to actively promote awareness of the TFTP and supports Member States seeking its advice and experience in devising Article 10 Requests. The Commission also encourages Member States to exploit to the full the possibilities available under the TFTP.

3.3. TFTP Provided Data accessed

Article 13 of the Agreement stipulates that the review should have a particular regard to, inter alia, the number of financial payment messages accessed.

As explained in Annex II and during the review, on the one hand, the same financial payment messages may respond to multiple searches needed in one or more investigations, while on the other hand, there are searches that return no results. 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. The overwhelming majority of messages that are accessed will never be disseminated; most will be viewed for a few seconds to determine their value and then closed, with no further action or dissemination. For these reasons, the most realistic and pragmatic way to measure the actual usage of TFTP data is to consider the number of searches run on the data.

During the review period, TFTP analysts conducted 27,095 searches of the TFTP, for an average of 1,232 searches per month as compared to 1,343 searches per month in the previous reporting period. 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.

The Treasury maintains its view that disclosure of overly 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 have the effect that terrorists would try to avoid such message types in those regions. It is not an obligation, under the Agreement, for the U.S. side to provide information on the volume of financial messages transferred under the Agreement.

As in the past, the Treasury agreed to provide trends giving some indications on the actual overall amount of data transferred without compromising the effectiveness of the TFTP. According to the information shared by the Treasury, the trend of the number of financial messages received from the Designated Provider has been slightly higher over the course of the 22 months of the review period. The increase was primarily the result of an increase in the volume of the message types responsive to the requests transiting the Designated Provider's system.

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

The Agreement gives an important role to Europol, which is responsible for receiving a copy of data requests, along with any supplemental documentation, and verifying that these U.S. requests for data comply with conditions specified in Article 4 of the Agreement, including that they must be tailored as narrowly as possible in order to minimise the volume of data requested. Once Europol confirms that the request complies with the stated conditions, the

data provider is authorised and required to provide the data to the Treasury. Europol does not have direct access to the data submitted by the data provider to the Treasury and does not perform searches on the TFTP data.

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 22 requests from the Treasury. The statistical information provided by Europol to the review team is attached as Annex III.

Given that the supporting documentation for Article 4 requests has continuously developed further from a quantitative and qualitative perspective, much of it in response to requests from Europol and the following up of recommendations made to Europol by the JSB, during the review period, Europol was not required to ask for supplemental information in order to complete its verification under Article 4 of the EU-US TFTP Agreement.

In addition to information received both orally and in writing from the Treasury and Europol, the review team examined two Article 4 requests' classified supporting documentation and on that basis discussed with the Treasury the procedures for the preparation and handling of their requests and scope.

The process for preparation, verification and validation of Article 4 requests by the Treasury remained the same as in the previous review. Taking into consideration the most recent terrorist threats and vulnerabilities, counter-terrorism analysts assess the scope of the request and update the supplemental documentation 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 provide 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’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.

Article 4 requests take into account the results of the Treasury's regular evaluation 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 is conducted every year, analysing 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 of the extracted data is conducted 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 conducted one such large-scale evaluation during the review period. In December 2014, the Treasury Department completed its comprehensive annual audit and analysis and determined that all of the message types and geographic regions included in its Requests were necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. The 2015 evaluation had not concluded by the end of the joint review period.

Europol outlined its well established verification process under Article 4 of the Agreement to the review team, which also includes obtaining advice from its Data Protection Officer. The assessment of security needs and operational considerations, on which the requests are based and against which the requirement for requests to be tailored as narrowly as possible is examined, remains core for an efficient verification. Europol, as a law enforcement agency, has the necessary knowledge and ability to cover these aspects.

The Commission acknowledges the benefits of the close cooperation between the U.S. authorities, Europol and EU counter-terrorism authorities in assessing and communicating on terrorism-related threats. No situation was identified in which the independence between the verification role under the Agreement and operational cooperation was impaired, also due to the fact that the verification process within Europol involves several internal actors (including the Data Protection Officer). It is important that such cooperation, while certainly desirable and beneficial, continues to remain distinct from Europol's verification role under Article 4 of the Agreement.

The review team considered the JSB Report of 9 September 2015, noting that the clear improvements in content, relevance, accuracy, accountability and readability of the Treasury's requests since the 2012 inspection have been maintained. The report states that Europol has adopted the recommendation made during the last inspection to adopt a retention policy for Article 4 requests and supplementary documentation and that such policy is implemented. The report notes that Europol continues to implement its task under the terms of the Agreement to the best of its abilities, in line with the JSB's recommendations.

The review team received information from the Designated Provider on the security measures put in place in order to ensure the protection of data that is subject to the Agreement. The Designated Provider also confirmed that it had not encountered any issues in relation to the transfer of data under the Agreement.

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

Based on the explanations and information provided by Europol and the Treasury during the review, and also from the Designated Provider, it can be concluded that Europol is fully accomplishing its tasks pursuant to Article 4.

Request for public access – Involvement of the European Ombudsman

In the previous reporting period, following Europol's decision not to grant public access to the classified part of the second inspection report of the JSB on Europol's handling of Article 4 requests (from 2012), a member of the European Parliament (EP) lodged a complaint with the European Ombudsman in 2013. Europol provided its observations to the European Ombudsman, including Europol's views on the case which are releasable to the complainant.

Europol informed the Commission that it is confident that the public access request was assessed in accordance with the applicable regulatory framework in a diligent manner, in consultation with the U.S. authorities (as data originator of the underlying classified information). The complainant's original application, as well as the confirmatory application for public access, were given thorough consideration. Accordingly, from Europol's perspective, there were no grounds to deviate from the original decision on the basis of the complaint, i.e. to uphold the decision to deny public access. In its reply to the Ombudsman Europol explained, contrary to the assumption expressed by the complainant, that the JSB did not agree to publish the classified part of the second inspection report, given that the JSB proposed to release the classified part of the inspection report to the LIBE Committee through 'restricted access', not to publish it (public access). Europol also highlighted to the Ombudsman that legal requirements and practical modalities for access by the European Parliament to classified information processed by Europol are not in force.

The European Ombudsman closed its inquiry on 2 September 2014. She submitted that, as the U.S. authorities refused Europol's request to allow the Ombudsman to inspect the JSB report, the Ombudsman has not been able to determine whether the content of the report justified the refusal to make the report public. It has therefore become impossible for the Ombudsman to inquire further into this case. The Ombudsman acknowledged that Europol has fully cooperated with her services throughout the inquiry. In particular, the Ombudsman notes that Europol did its utmost to convince the U.S. authorities of the necessity for the Ombudsman to inspect the document concerned.

3.5. Monitoring safeguards and controls – the role of 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 the Provided Data is only processed in accordance with the Agreement. These safeguards are intended to ensure that only the data responsive to specific and justified searches on the subjects with a nexus to terrorism and its financing is actually accessed. This means in practice that while all data provided pursuant to Article 4 is searched, only a small proportion of the data is actually viewed and accessed. Therefore the data of persons not retrieved in a specific counter-terrorism search will not be accessed.

The review team verified that the safeguards described in Article 5 have been put in place and function as intended. To this end, the review team also checked a representative sample of searches selected in advance of the review and found no instances of non-compliance with the provisions of the Agreement. In addition, the review team specifically looked at the functioning of the oversight mechanism described in Article 12.

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 Commission is satisfied that data is processed exclusively for the purpose of preventing, investigating, detecting or prosecuting terrorism or its financing (Article 5 (2)).

The 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 highlighted the fact 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.

The review team had the opportunity to speak to both the Designated Provider's and the EU's overseers. The review team was informed that the overseers verify all 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 retroactively 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: all overseers, including the overseers appointed by the EU, had requested additional information on an on-going basis and also blocked searches. The overseers performed real-time and retrospective reviews. It was confirmed to the review team that, even in cases of retrospective review, the Treasury does not disseminate any data before the overseers have completed their scrutiny procedures.

During the review period the overseers verified all 27,095 searches conducted by the analysts, queried 450 searches and blocked 45 searches, the search terms of which were considered to be too broad. The overseers verified the majority of the searches as they occurred and all of the searches, including those reviewed as they occurred, within one working day.

The overseers work in a complementary way by supporting each other in order to accomplish their tasks. The fact that a search has been selected for scrutiny by one of the overseers is visible to the other overseers, who would generally not select the same search in order to avoid the duplication and maximize the efficiency of the oversight. For this reason the information about the searches queried and blocked by the overseers was provided as a total figure in Annex II.

In 2013, the Commission and the Treasury agreed on measures further supporting the role of the EU overseers. The EU overseers since then have the opportunity to:

- discuss general developments, day to day cooperation and any operational matters relating to the TFTP during the quarterly meetings with the management of the Treasury;

- receive quarterly threat briefings on terrorist financing methods, techniques and operations relevant to the TFTP in order to have up-to-date knowledge useful for the fulfilment of their function;

- discuss the results of the Designated Provider's oversight and audit functions during the quarterly and ad-hoc meetings.

The Commission is satisfied that the oversight mechanism is functioning smoothly and is effective in ensuring that the processing of data complies with the conditions laid down in Article 5 of the Agreement.

3.6. Data security and integrity – independent audit

The review team visited the location where TFTP-related searches are carried out and data is handled. In addition, questions related to this issue in the questionnaire – as well as those raised orally in the course of the on-site visit – were replied to comprehensively and convincingly by the Treasury.

The review team had the opportunity to speak to a representative of the Designated Provider responsible for auditing procedures to test data security and integrity which give additional assurances as to the compliance of the TFTP with the provisions of the Agreement. He provided a detailed presentation and replied to all subsequent questions raised by the team.

Based on all this, the Commission considers the measures taken to ensure data security and integrity as satisfactory. The various presentations to the joint review team demonstrate that utmost care has been and is being taken by the U.S. authorities to ensure that the data is held in a secure physical environment; that access to the data is limited to authorised analysts investigating terrorism or its financing and to persons involved in the technical support, management, and oversight of the TFTP; that the data is 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, no copies of the Provided Data can 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. They also closely monitor and verify the deletion processes. These auditors report back to the Designated Provider every three months, including on whether there have been any discrepancies or atypical occurrences related to the data traffic.

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

3.7. Retention and deletion of data

The review team received detailed explanations on the deletion process and its challenges 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. The deletion process is closely monitored and verified by the independent auditors' representative. For these reasons this complex deletion exercise cannot be implemented as an automated process.

In order to fully comply with provisions of Article 6 (4) of the Agreement and in response to the recommendation of the second joint review, the Treasury now deletes the data on a semi-annual basis in order to ensure that all non-extracted data is deleted at the latest five years from receipt. All non-extracted data received prior to 31 December 2010 had already been deleted at the time of the review, well ahead of the due date.

Article 6 (1) requires that the Treasury should undertake an ongoing and at least annual evaluation to identify non-extracted data that is no longer necessary to combat terrorism or its financing. Where such data is identified, the Treasury should delete it as soon as technologically feasible.

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. The Treasury assesses the data retention periods as part of the regular evaluation of the extracted data received described under 3.5 which includes investigators' interviews, reviews of counter-terrorism investigations, and an evaluation of current terrorist threats and activity. Based on its results, the Treasury is of the view that the current retention period is appropriate. The Joint Value Report adopted by the Commission on 27 November 2013 concluded that the reduction of the TFTP data retention period to less than five years would result in a significant loss of insights into the funding and operations of terrorist groups.

According to Article 6 (7), the information extracted from the Provided Data, including information shared under Article 7, shall be retained for no longer than necessary for specific investigations or prosecutions for which they are used. The review team discussed with the Treasury the reasonable and efficient implementation of this provision, which does not impose a specific retention period.

The Treasury explained that, with regard to the disseminated information, it notifies law enforcement and intelligence agencies that receive leads derived from the TFTP data to retain them for a period no longer than is necessary for the purpose for which they were shared. Furthermore, counter-terrorism analysts using the TFTP receive training on the safeguards, dissemination, and retention procedures required by the Agreement prior to use of the system. In addition, U.S. Government agencies are obliged to develop and implement retention schedules describing the disposal of their records.

As regards the extracted data retained in the TFTP database, the Commission recommended during the previous joint review that this aspect be included and specified in the Treasury's instructions for the regular evaluations and continue to be monitored in the future.

The Treasury informed the review team that data extracted in the context of its operations are subject to the records disposition schedule of the Office for Foreign Assets Control. The Treasury assesses the necessity of retaining extracted data in the sense of Article 6 (7) during its regular evaluations described under 3.4., and in relation to, inter alia, ongoing investigations and prosecutions.

In light of the information provided by the Treasury, the Commission is satisfied that retention and deletion of data pursuant to Article 6 is satisfactorily implemented.

3.8. Transparency – 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. The website also contains a document containing questions and answers about the TFTP, which was last updated in March 2016.

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 includes the possibility of leaving a voicemail message. The 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, none of the recorded voicemail messages were related to the TFTP. Treasury personnel responded to several emails received in the assigned e-mail account (tftp@treasury.gov) containing questions about the scope of the TFTP.

3.9. Right of access and to rectification, erasure, or blocking

Upon the entry into force of the Agreement, the Treasury set up procedures for individuals to seek access to their personal data under the TFTP Agreement and to exercise the rights to rectification, erasure or blocking of their personal data under the Agreement. These procedures are described in Annex II and can also be found on the Treasury website. They have to comply with US national law as well as the Agreement.

During the review period, the Commission and the Treasury continued working together and in cooperation with the EU's Article 29 Working Party to establish uniform verification procedures and common templates to be applied by all National Data Protection Authorities (NDPAs) when receiving the requests from EU citizens. These procedures have been agreed upon and put in place as of 1 September 2013. Prior to that the Article 29 Working Party informed all its members and requested that they make the information and the forms available on their respective websites.

During the current review period, the Treasury Department identified and shared with the Commission certain refinements to the procedures that may facilitate the prompt receipt of requests from the NDPAs by Treasury. The Commission will continue to work with the Treasury to further improvements to the procedures.

3.9.1. Requests for access

Pursuant to Article 15 (1) of the Agreement, any person has the right to obtain at least a confirmation transmitted through his or her NDPA as to whether that person's data protection rights have been respected in compliance with the Agreement and, in particular, whether any processing of that person's personal data has taken place in breach of this Agreement. This does not provide for the right of persons to receive a confirmation as to whether that person's data has been amongst the TFTP Provided Data. Otherwise, Provided Data not previously accessed in the course of a terrorism-related investigation would have to be accessed, and that would be considered a breach of the purpose limitation provisions of the Agreement.

During the review period, the Treasury received three perfected requests through European NDPAs, wherein an individual sought to exercise the provisions described in Article 15 of the Agreement. In each of the three cases, the Treasury Department provided responses to the European NDPAs, confirming that the requester’s data protection rights have been respected in compliance with the TFTP Agreement. On 15 March 2016, there were no perfected requests pursuant to Article 15 or 16 of the TFTP Agreement pending with the Treasury.

The Treasury explained to the review team the process and the technical aspects of preparing a responsible and correct response to a request. When verifying whether the data of the requester have been accessed, the Treasury needs to ensure strict compliance with the Agreement's safeguards. During the process monitored and verified by the independent auditors' representative, the Treasury would review all search logs and extracted data in order to respond on whether the requester's data protection rights have been respected in compliance with the Agreement and in particular whether any processing of that person's data has taken place in breach of the Agreement in accordance with Article 15 (1). The review team and the Treasury also discussed how to apply reasonable limitations foreseen in Article 15 (2).

As stated in the previous joint review report, the Commission has continued the discussion on the interpretation of Article 15 concerning the right of access. The Commission acknowledges that individual investigations, as well as the TFTP as such, could be compromised if the Treasury had to respond to individuals about whether their data has been processed in the context of searches in the TFTP.

In light of the information provided by the Treasury, the Commission is satisfied that the right of access pursuant to Article 15 is satisfactorily implemented.

3.9.2. Requests for rectification, erasure, or blocking

Article 16 (1) of the Agreement provides for the right of any person to seek the rectification, erasure, or blocking of his or her personal data processed by the Treasury pursuant to the Agreement where the data is inaccurate or the processing contravenes the Agreement.

No requests for rectification, erasure or blocking of personal data under the TFTP had been received by the Treasury by the time of the review.

In response to the recommendation of the second review, the Treasury included information about the implications of Article 5 (4) (d), which forbids any manipulation, alteration, or addition of the TFTP Provided Data, on the process of rectification in the TFTP questions and answers document published on the Treasury website[9].

3.10. Redress

According to Article 18, individuals have several possibilities for redress, both under European law and under U.S. law. During the review, only the U.S. redress mechanism was discussed. Since the entry into force of the Agreement there has not been any case of a claim for redress addressed to the U.S., so the possible options have not been asserted in practice.

The Agreement provides that any person who considers his or her personal data to have been processed in breach of the Agreement may seek effective administrative or judicial redress in accordance with the laws of the EU, its Member States, and the United States, respectively. The United States has agreed that the Treasury should treat all persons equally in the application of its administrative process, regardless of nationality or country of residence.

Subject to Article 20 (1), the Agreement provides for persons, regardless of nationality or country of residence, to have available under U.S. law a process for seeking judicial redress from an adverse administrative action. Relevant statutes for seeking redress from an adverse Treasury administrative action in connection with personal data received pursuant to the Agreement may include the Administrative Procedure Act and the Freedom of Information Act. The Administrative Procedure Act allows persons who have suffered harm as a result of certain U.S. Government agency actions to seek judicial review of such actions. The Freedom of Information Act allows persons to utilize administrative and judicial remedies to seek government records. According to the Treasury, an EU citizen or resident may seek judicial redress from an adverse administrative action by filing a complaint with a court in an appropriate venue.

The review team was informed of the adoption in February 2016 of the so-called 'Judicial Redress Act of 2015', which –subject to designation from the U.S. Attorney General- extends to EU citizens core benefits of the 1974 Privacy Act. EU citizens will have legal standing before U.S. Courts to file lawsuits in cases of refused access, rectification or unlawful

[9] https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/tftp_brochure_03152016.pdf

disclosure of their personal data. This will also supplement the possibilities for judicial redress already provided for by the TFTP Agreement.

3.11. Consultations under Article 19

In reaction to the 2013 media allegations about the U.S. possibly accessing SWIFT data outside the Agreement, the Commission initiated formal consultations as a framework to assess whether the implementation of the Agreement might have been affected. The U.S. side provided explanations and gave written reassurances that the U.S. Government has not, since the entry into force of the Agreement, collected financial payment messages from the Designated Provider in the EU except as authorised by the Agreement. In this context then European Commissioner for Home Affairs Cecilia Malmström and former U.S. Treasury Under Secretary for Terrorism and Financial Intelligence David Cohen agreed to intensify efforts to keep the implementation of the Agreement under close scrutiny and agreed on some concrete measures to achieve this, including measures further supporting the role of the EU independent overseers[10].

During the consultations the Commission also conducted a dialogue with the Designated Provider to determine whether its data had been accessed by the U.S. contrary to the Agreement. Separately, the General Counsel of the Designated Provider was invited by the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) of the European Parliament to make a statement to its Inquiry on electronic mass surveillance of EU citizens. More detailed information is provided below.

On 27 November 2013, Commissioner Malmström informed the European Parliament about closing the consultation process, which had not revealed any elements indicating a breach of the Agreement. The results of this review provide further assurances that the Agreement has been properly implemented by the U.S. side.

In reply to the specific question of the EU review team (question 12 in Annex II), the Treasury confirmed the validity of the assurances given during the consultations. It stated that since the TFTP Agreement entered into force in August 2010, the U.S. Government – including all departments and agencies – has not collected financial payment messages from the Designated Provider in the European Union, except as authorized by the TFTP Agreement. The Treasury also stated that, during that time, the U.S. Government has not served any subpoenas on the Designated Provider in the EU or on the Designated Provider in the United States requesting the production of data stored in the EU, except as authorized by Article 4 of the TFTP Agreement. The Treasury also confirmed that the United States has remained and intends to remain in full compliance with all of its commitments under the TFTP Agreement.

At the end of 2013, the Dutch and the Belgian data protection authorities opened an investigation into the security of financial messaging data at the Designated Provider, in part due to the reports in international media that foreign intelligence services allegedly had unlawful access to financial messaging data at the Designated Provider. On 8 May 2014, the

[10] http://europa.eu/rapid/press-release_IP-13-1160_en.htm

two data protection authorities concluded that during their investigation into the security of the computer networks of the Designated Provider, they did not find any violations of legal security requirements. The investigating data protection authorities also had no indications that third parties have had or could have had unlawful access to financial messaging data related to European citizens[11].

Statement by the Designated Provider on its security protection

On 24 September 2013, the General Counsel of the Designated Provider informed the Inquiry on electronic mass surveillance of EU citizens of the LIBE Committee that the Company had no evidence to suggest that there has ever been any unauthorised access to its systems or data and provided explanations about the security protection in place. The relevant elements of the Statement are described below.

The Designated Provider operates its services to the highest data protection and security standards, as security is of the utmost importance to its customers. To achieve this objective, the messages and data flows are encrypted and logical security and physical security requirements are identified, implemented and continuously monitored. Concrete examples of how the Designated Provider builds its defensive security architecture for its critical systems and services were also presented.

The Designated Provider has a structured and tiered internal network infrastructure which ensures that servers and data are shielded away from threats, whether internal or external. Its network is isolated from the pure Internet. All external network accesses are restricted and internal duties strictly segregated. Tight network controls are imposed and strong security baselines operated on.

The Designated Provider has also deployed a set of deterrence and detective controls, including, inter alia, intrusion-detection systems and protected logging, application-specific correlation capabilities and network behaviour analysis tools. The Designated Provider has an intrusion-testing programme including logical and physical security, as well as social engineering aspects and a process in place to help ensure that findings are prioritised so that appropriate and timely actions are taken accordingly. This programme covers all exposed components of the service delivery, from network to application level.

The Designated Provider has defined strict guidelines for the maintenance, repair and disposal of equipment or media such as computers with hard disks, disk units, and other storage media to ensure that data cannot be recovered. Rigorous staff vetting procedures are in place, which include background screening, reference checking and maintaining security awareness through on-going training and communication programmes.

Physical access to the Designated Provider's premises, computer equipment, data storage and resources is restricted. The operating centres are designed to house mission-critical computer

[11] http://www.dutchdpa.nl/Pages/en_pb-20140508-swift-bank-data-security.aspx

operations. Physical security controls are in place to prevent, deter, detect and delay penetration. The perimeters around the operating centres are enclosed, guarded and monitored. Access tokens and associated Personal Identification Numbers or Biometrics exist for doors and provide audit trails of access to computer floors.

Finally the Designated Provider's security, including the processes and technical controls in place to ensure its customers' data protection, is subject to multiple levels of oversight.

4. RECOMMENDATIONS AND CONCLUSION

On the basis of the information and explanations received from the Treasury, Europol, the Designated Provider and the independent overseers, verification of relevant documents and of a representative sample of the searches run on the TFTP provided data, the Commission is satisfied that the Agreement and its safeguards and controls are properly implemented and that the findings of the third joint review have been followed up by the Treasury.

In its written reply to the questionnaire (Annex II), the Treasury confirmed the validity of the assurances given during the 2013 consultations. In particular, it restated that since the TFTP Agreement entered into force in August 2010, the U.S. Government – including all departments and agencies – has not collected financial payment messages from the Designated Provider in the European Union, except as authorized by the TFTP Agreement.

The Commission welcomes the efforts made by the Treasury to collect, analyse and make available to the review team and to the public examples demonstrating the important value of the TFTP for counter-terrorism investigations worldwide, despite the limitations given by the highly sensitive nature of these investigations. The detailed information about how the TFTP Provided Data can and is being used and various concrete cases thereof provided in the Joint Value Report and in the context of this review constitute a considerable step forward in further explaining the functioning and the added value of the TFTP.

The Commission acknowledges the benefits of the close cooperation between the U.S. authorities, Europol and EU counter-terrorism authorities in assessing and communicating on terrorism-related threats ensuring that the TFTP also addresses the threat from the EU perspective. Europol is fully accomplishing its tasks pursuant to Article 4. It is important that such cooperation continues to remain independent from the verification role of Europol under Article 4 of the Agreement.

The Commission suggests that the Member States consider providing regular feedback on the TFTP data received from the Treasury which could further improve the quality and the quantity of information exchanged under Articles 9 and 10. In addition, the Commission encourages Europol to continue its efforts to actively promote awareness of the TFTP and to support Member States seeking its advice and experience in devising Article 10 requests.

A regular review of the Agreement is essential to ensure its proper implementation, to build up a relationship of trust between the contracting parties and to provide reassurances to interested stakeholders on the usefulness of the TFTP instrument. It has been agreed between

the Commission and the Treasury to carry out the next joint review according to Article 13 of the Agreement in the beginning of 2018.

ANNEX I

COMPOSITION OF THE REVIEW TEAMS

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

– Luigi Soreca, Director Internal Security, Directorate-General Migration and Home Affairs, European Commission – Head of the EU review team;

– Jeroen Blomsma, Unit D2 – Terrorism and Radicalisation, Directorate-General Migration and Home Affairs, European Commission;

– Frédéric Claeys, expert on data protection, Legal Advisor, Belgian Privacy Commission;

– Péter Kimpián, expert on data protection, Hungarian National Authority for Data Protection and Freedom of Information;

– Francisco Jiménez-Villarejo, vice-president and national member for Spain, Eurojust

It is noted that Frédéric Claeys and Péter Kimpián participated in the EU review team as experts for the Commission and not in their other professional capacities.

The members of the **U.S. team** were:

– Michael Mosier, Associate Director, Office of Foreign Assets Control, U.S. Department of the Treasury – Head of the US review team;

– Holly Phelps, Coordinator for Operational Programs, Office of Foreign Assets Control, U.S. Department of the Treasury;

– M. William Schisa, Senior Counsel, Office of the Chief Counsel (Foreign Assets Control), U.S. Department of the Treasury;

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

– Jocelyn A. Aqua, Senior Component Official for Privacy, National Security Division, U.S. Department of Justice;

– Robert Gerber, Economic Officer, Office of European Union Affairs, U.S. Department of State;

– Michael Olmsted, Senior Counsel for the European Union and International Criminal Law Matters, U.S. Mission to the European Union.

ANNEX II

U.S. TREASURY DEPARTMENT RESPONSE TO

EU QUESTIONNAIRE

FOR THE FOURTH JOINT REVIEW OF THE EU-U.S. TFTP AGREEMENT

(MARCH 2016)

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

The first joint review carried out in February 2011 covered the period of the first six months after the entry into force of the Agreement (1 August 2010 until 31 January 2011) and the second joint review covered the ensuing period from 1 February 2011 until 30 September 2012. The third joint review covered the period from 1 October 2012 until 28 February 2014. The fourth joint review will cover the period from 1 March 2014 to 31 December 2015.

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; and*

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."*

II. Statistical information

1. **In comparison to the period covered by the first three joint reviews, 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 higher over the course of the 22-month period between 1 March 2014 and 31 December 2015 ("the review period"). The increase is primarily the result of an increase in the volume of the message types responsive to the Requests transiting the Designated Provider's system.

2. **How many financial payment messages were accessed (i.e., extracted) during the period covered by the review?**

During the 22 months of the review period, TFTP analysts conducted 27,095 searches of the TFTP, for an average of 1,232 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 competent authorities in the EU and third-countries, what is the trend of information derived from accessing these payment messages provided to competent U.S. authorities (substantially/slightly higher/lower, about the same)?**

The trend of TFTP-derived information provided to EU and third-country authorities has increased substantially during the review period, due to terrorist attacks in Europe in 2015 and the increased terrorist threat to the EU as a whole. Please see the responses to Questions 4, 5, 10, and 11, below. The Treasury Department provided TFTP-derived information to competent U.S. authorities at about the same rate as the prior review period, in connection with ongoing U.S. counter-terrorism investigations.

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

During the 22 months of the current review period, U.S. investigators supplied 93 TFTP-derived "reports" consisting of 2,680 leads pursuant to Article 9 and an additional 8,998 "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 147 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 2,300 TFTP reports have been provided to the EU Member States and Europol in the 14 years since the program began. During the 22 months of the current review period, 11,678 TFTP leads were provided to EU Member States and Europol.

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

U.S. investigators supplied 53 reports consisting of 383 leads resulting from TFTP data to competent authorities of third countries during the 22 months of the current review period. 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 3,350 such reports have been provided to competent authorities throughout the world since the program began, the majority of which (more than 2,300 such reports, plus an additional 8,998 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 United States 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, the Second Joint Review in October 2012, and the Third Joint Review in April 2014. Other sensitive and non-public TFTP-derived information was shown to officials from certain EU institutions, such as 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 accept the TFTP-derived information as supporting or indirect evidence?**

Article 7(c) provides that TFTP-derived 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-derived information in a criminal trial. Instead, the authorities must use the TFTP-derived information as a means to gather the evidence that may properly be presented to a judicial authority in a proceeding. The Treasury Department does not and could not track where authorities may have used counter-terrorism lead information derived from the TFTP as a means to gather evidence that might be used in a judicial proceeding. The Treasury Department is aware, however, that TFTP-derived information has been used with some frequency by U.S. and other counter-terrorism investigators for lead purposes to support their investigations, including in connection with obtaining evidence through legal process. The Treasury Department also requests examples where TFTP-derived information was used in a counter-terrorism investigation, some of which are cited in the attached paper.

10. **In how many cases was information provided spontaneously, in accordance with Article 9 of the Agreement? What has been the U.S. Treasury's experience with receiving follow-on information conveyed back by Member States, Europol or Eurojust?**

During the 22 months of the review period, 93 reports consisting of 2,680 TFTP leads were provided to EU Member States and Europol as the spontaneous provision of information pursuant to Article 9.

Following the January and November 2015 terrorist attacks in France, the Treasury Department received positive feedback from Europol and certain EU Member States about the value derived from the Treasury Department's provision of TFTP-derived information.

However, it is uncommon for EU Member States or Europol to provide the Treasury Department with analytic "follow-on information" in response to the provision of information pursuant to Articles 9 and 10. The Treasury Department welcomes Europol's ongoing efforts to encourage EU Member States to provide feedback, where possible, to the Treasury Department, and continues to believe 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.

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? In how many cases was there a feed-back to the U.S. Treasury Department on that information coming from EU-MS or Agencies?**

The Treasury Department received 192 requests from EU Member States and Europol pursuant to Article 10 during the review period and has responded to all requests.[12] TFTP searches resulted in the transmission of leads to the EU in response to 121 of the 192 requests. There were 8,998 leads contained in the 121 Article 10 responses provided to EU Member States and Europol during the review period. In four cases, the Treasury Department received feedback from EU Member States through Europol after submitting an Article 10 response.

III. Implementation and effectiveness of the Agreement

12. **Can you confirm that the assurances given by the U.S. Treasury Department during the consultations carried out under Article 19 of the Agreement in 2013 are still valid and that the U.S. has remained and will remain in full compliance with the Agreement?**

Yes. Since the TFTP Agreement entered into force in August 2010, the U.S. Government – including all departments and agencies – has not collected financial payment messages from SWIFT in the European Union, except as authorized by the TFTP Agreement. Moreover, during that time, the U.S. Government has not served any subpoenas on SWIFT in the EU or on SWIFT in the United States requesting the production of data stored in the EU, except as authorized by Article 4 of the TFTP Agreement. The Treasury Department confirms that the United States has remained and intends to remain in full compliance with all of its commitments under the TFTP Agreement.

[12] The Treasury Department notes that, due to the timing of some of the 192 requests, some of the responses were provided to Europol after the conclusion of the review period.

13. **During the period covered by the review, 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?**

No.

14. **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 generally submitted its Article 4 Requests on a monthly basis. On three occasions in 2015, the Treasury Department submitted two Requests in the same month, with no Request in the following month. In each instance, Treasury did so either at the request of the Designated Provider or to accommodate the potential disruption posed by the possibility of a temporary shutdown of the U.S. Government.

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.

15. **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 conducted one such large-scale evaluation during the review period. In December 2014, the Treasury Department completed its comprehensive annual audit and analysis and determined that all of the message types and geographic regions included in its Requests were necessary for the purpose of the prevention, investigation,

detection, or prosecution of terrorism or terrorist financing. The 2015 evaluation had not concluded by the end of the joint review period.

The Treasury Department will continue to conduct additional necessity-based reviews to ensure that the Requests remain tailored as narrowly as possible based on past and current terrorism risk analyses.

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

Europol 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.

17. **In how many cases has Europol requested supplemental information for the requests under Article 4(1)? Have there been any cases in which Europol came to a conclusion 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). During the 22-month review period, Europol also did not request supplemental information from the Treasury Department with respect to Requests submitted pursuant to Article 4(1) in order to verify the sufficiency of the 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.

In an ongoing effort to enhance the Requests beyond the requirements set out in Article 4(2), Europol officials regularly provided comments and suggested that the Treasury Department include additional information to improve the clarity and focus of the Requests. The Treasury Department carefully considered these suggestions and generally incorporated them in subsequent Requests.

18. **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 increasingly important and effective in supporting European and global counter-terrorism efforts, particularly in light of the heightened terrorist threat to Europe during the review period. In response to requests related to the November 2015 attacks in Paris, the Treasury Department provided over 800 TFTP-derived leads to European authorities in support of ongoing investigations. Europol Director Wainwright specifically noted the value of TFTP-derived information to French investigations in testimony before the European Parliament on 19 November 2015. Similarly, in response to requests related to the January 2015 terrorist attack in Paris and the anti-terrorism raid in Verviers, the Treasury Department was able to provide over 580 leads to

Europol and other European counter-terrorism authorities. Notably, the Treasury Department responded to the first requests related to the kosher market incident while the hostage crisis was still ongoing.

The Treasury Department has identified no specific impediments to achieving the stated purpose of the Agreement, and continues to engage directly with European authorities, including Member States and Europol, to improve the awareness and usage of the TFTP Agreement among relevant authorities.

19. **Is the TFTP subject to oversight by U.S. authorities? If so please elaborate. What is the role of U.S. Congress within this mechanism?**

In addition to the multiple, mutually reinforcing data safeguards provided by the EU-appointed overseers and the independent, external overseers, the TFTP is subject to multiple layers of oversight by U.S. authorities. The Treasury Office of the Inspector General ("OIG") provides independent oversight of the programs and operations of the Department of the Treasury pursuant to its statutory authorities and consistent with Article 12(2) of the TFTP Agreement. The OIG has fulfilled and continues to fulfill its responsibilities regarding independent oversight with respect to the TFTP, including monitoring the deletion of certain data pursuant to Treasury's commitments in Article 6. The OIG concluded that this data deletion was conducted in accordance with the U.S.-EU TFTP Agreement.

In addition to the OIG, the Treasury Department's Office for Privacy, Transparency, and Records provides verifications regarding the Treasury Department's implementation of the TFTP Agreement. The Office of General Counsel is also closely involved in ensuring the Treasury Department implements the TFTP in accordance with the terms of the Agreement. For more information, please see the response to Question 20, below.
Furthermore, 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 Committees on these issues.

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

20. **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 an EU National Data Protection Authority ("NDPA"), acting on behalf of a person, submit a request in writing to the Treasury Privacy Officer pursuant to Articles 15 and/or 16 of the Agreement. Prior to submitting a request, the NDPA must obtain proof of the requestor's identity in order to ensure that there are no unauthorized disclosures of personal data. After obtaining proof of the identity of the person making the request, the NDPA must send (preferably via a method of delivery that allows tracking) to the Treasury Privacy Officer the original access request form and/or the rectification, erasure, or blocking request form and the waiver form (all completed in English), together with a signed copy of the standard request letter. Upon sending the request, the NDPA must notify the Treasury Privacy Officer via email that the request is in transit. Once the Treasury Privacy Officer receives a request via regular mail with all of the required information (a "perfected request"), the Privacy Officer processes the request as follows: (1) notify the NDPA of receipt of the perfected 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,[13] along with the Inspector General of the Treasury Department, have oversight with respect to the entirety of the program.

21. **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 prior review period, Treasury Department officials worked constructively with the Commission, which consulted on this topic with the EU's Article 29 Working Party, to establish uniform procedures, whereby the verification of identity of EU 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. The Article 29 Working Party applied the finalized procedures in all member countries as of 1 September

[13] 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.

2013, at which point the Treasury Department began to accept Articles 15 and/or 16 verification decisions by EU NDPAs.

During the current review period, the Treasury Department identified and shared with the Commission certain refinements to the procedures that may facilitate the prompt receipt of requests from the NDPAs by Treasury. The Treasury Department will continue to work with the Commission to make any additional adjustments required as these procedures are implemented. For more information, please see the responses to Questions 41 and 42, below.

22. **Have any of the 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?**

There have been no changes to the implementation of the Article 5 safeguards during the review period. The team of Commission-appointed overseers continues to carry out the functions related to the Article 5 safeguards and has all of the necessary access to fully review all TFTP searches in real-time and is an integral part of the implementation of the data safeguards embedded in the TFTP.

The comprehensive and multilayered set of systems and controls previously reviewed remains 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 fulfillment 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.

23. **Have any of the 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 22, 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.

24. **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 no changes have been made since the last joint review.

25. **What is the policy for log files (which data processing activities are logged, who has access, is there any monitoring procedure in place, what is the retention period foreseen for logs)?**

In accordance with Articles 5(6) and 7(f) of the TFTP Agreement, the Treasury Department maintains logs of individual TFTP searches, including the nexus to terrorism or its financing required to initiate the search, and of the onward transfer of TFTP-derived information. TFTP search log files may be subject to review by scrutineers or auditors, and are retained for audit and compliance purposes, in accordance with U.S. Government records retention requirements. Please see the response to Question 22, above, and Question 35, below.

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 the response to Question 22, 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 ongoing 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 the response to Question 15, 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 a semiannual deletion process. This deletion has occurred with respect to all data received in response to message types or geographic regions removed from the Request.

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 31 December 2010 been deleted as provided for in Article 6(4) of the Agreement?**

Yes. All non-extracted data received prior to 31 December 2010 were deleted prior to 31 December 2015, in accordance with Article 6(4) of the Agreement.

31. **Have any measures taken to provide for the ongoing 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 15, above. A comprehensive assessment consisting of investigator interviews, reviews of counter-terrorism investigations, and an evaluation of current terrorist threats and activity is conducted regularly to ensure that TFTP data retention periods are relevant to ongoing counter-terrorism efforts. Based on the four annual evaluations completed since the Agreement entered into force, as well as the ongoing assessments, 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. **Have there been any cases where these retention periods have been reduced by the U.S. Treasury Department in accordance with Article 6(5)?**

No. See the responses to Question 31, above, and 33, below.

33. **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? What is the process for deletion of such data?**

Treasury conducts an exhaustive semiannual evaluation to ensure that any non-extracted data received on or after 20 July 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 a semiannual basis could significantly impair the functioning of the system and be technologically infeasible.

The Treasury Department initially had intended to implement this provision via an annual deletion exercise, since automatic deletions of non-extracted data could result in the inadvertent deletion of extracted data necessary for specific ongoing counter-terrorism investigations and would not allow for the necessary controls and independent assessments to ensure that the appropriate data had been deleted. Following conversations during the second joint review, and at the recommendation of the EU joint review team, the Treasury Department revised its procedures to accommodate additional deletion exercises to ensure that all deletions of non-extracted data are fully completed by the five-year mark. Thus, all non-extracted data received prior to 30 June 2011 already have been deleted.

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. This is consistent with the legal requirement that U.S. Government agencies develop and implement retention schedules describing the disposal of their records. Furthermore, counter-terrorism analysts using the TFTP receive training on the safeguards, dissemination, and retention procedures required by the TFTP Agreement prior to use of the system.

The Treasury Department also continues to assess the necessity of the retention of extracted data pursuant to Article 6(7) of the TFTP Agreement. These assessments are completed as part of the review of extracted data described in response to Question 15, above. The retention and deletion of extracted data are consistent with OFAC's records retention schedule, as filed with the U.S. National Archives and Records Administration ("NARA"). OFAC's retention schedule is publicly available on NARA's website at http://archives.gov.

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 required by the TFTP Agreement 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. **Please describe how requests for subsequent dissemination of original TFTP-derived information are handled. Have any of these requests been rejected?**

As a general matter of policy, the Treasury Department requires recipients of TFTP-derived information to request additional dissemination approval from the Treasury Department, although in certain circumstances, such as when providing information to Europol, the Treasury Department allows the information to be further provided to competent authorities (particularly since Europol often acts as an intermediary between EU Member States and the U.S. Treasury Department). In all cases, however, the Treasury Department includes a warning containing the use limitations of the TFTP-derived data, including that the information may only be used for counter-terrorism lead purposes. When the Treasury Department receives a dissemination request that appears to be improper (e.g., the counter-terrorism mandate of the receiving agency is unclear), the Treasury Department generally works with the requesting agency to obtain clarifications with respect to the request. In situations where the request cannot be clarified, the requesting agency generally withdraws the request.

37. **Have all searches run on the TFTP data been subject to oversight defined in Article 12(1) of the Agreement?**

Yes.

38. **How many searches have been queried by the overseers? On which basis did the overseers select a search for further verification?**

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 450 searches – the overwhelming majority of which were selected for routine auditing purposes. All searches queried by the overseers are blocked until any overseer 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. The overseers blocked 29 searches at the time of the search and 16 additional searches during their retrospective review of the search logs because they believed the search terms were too broad. Blocked searches accounted for a small number of cases (45 total searches during the 22 months of the review period – or .0016 percent of all searches). 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 450 searches queried, the Treasury Department cannot accurately break them down between the Designated Provider and the EU overseers, because when one party queried a search, it was treated as queried by the overseers generally.

39. **In how many cases have the overseers blocked searches on the grounds that they appear to be in breach of Article 5 of the Agreement? Can any typical kind of search be identified where blocking was deemed necessary? Were there any other measures envisaged or taken?**

As noted in response to Question 38, above, in a small number of cases (45 searches during the 22 months of the review period – or .0016 percent), the overseers blocked the searches because they believed the search terms were too broad. While all of the searches blocked during the review period were deemed to be overly broad, the overbreadth may simply result from, for example, a typographical error in the spelling of a terrorism suspect's name or the transposition of two digits in a bank account number.

As noted in response to Question 22, above, all analysts who have access to the TFTP system are extensively trained and re-trained regularly to ensure the fulfillment of all requirements for searches. When an analyst attempts a search that does not satisfy the requirements, the Treasury Department has responded appropriately, including mandating additional training for the analyst and temporarily suspending the analyst's access rights to the TFTP until overseer concerns with the search are fully resolved. The Treasury Department may also permanently revoke an analyst's access rights to the TFTP or institute disciplinary proceedings, although the Treasury Department has not needed to exercise these options to date.

40. **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.

41. **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?**

As noted in the response to Question 21, above, during the current review period, the Treasury Department received three perfected requests through European NDPAs during the current review period, wherein an individual sought to exercise the provisions described in Article 15 of the Agreement. In each of the three cases, the Treasury Department provided responses to the European NDPAs.

The Treasury Department received no requests pursuant to Article 16 of the TFTP Agreement during the review period, and as of 15 March 2016, there are no perfected requests pursuant to Article 15 or 16 of the TFTP Agreement pending with the Treasury Department.

42. **Have those access requests been answered positively? In case where an exception was used for not providing a positive answer what was the procedure followed, what was the content of the answer provided to the data subject ?**

In each of the three perfected requests pursuant to Article 15 of the Agreement received and processed by the Treasury Department during the review period, the Treasury Department confirmed that the requester's data protection rights have been respected in compliance with the TFTP Agreement.

43. **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.

44. **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.

45. **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.

46. **How would a process of seeking administrative and judicial redress provided for in Article 18(2) by an EU citizen or resident look like?**

The TFTP Agreement provides that any person who considers his or her personal data to have been processed in breach of the Agreement may seek effective administrative or judicial redress in accordance with the laws of the EU, its Member States, and the United States, respectively. The United States has agreed that the Treasury Department shall treat all persons

equally in the application of its administrative process, regardless of nationality or country of residence.

The TFTP Agreement provides for persons, regardless of nationality or country of residence, to have available under U.S. law a process for seeking judicial redress from an adverse administrative action. Relevant statutes for seeking redress from an adverse Treasury Department administrative action in connection with personal data received pursuant to the TFTP Agreement may include the Administrative Procedure Act, the Freedom of Information Act, and the Judicial Redress Act. The Administrative Procedure Act allows persons who have suffered harm as a result of certain U.S. Government administrative actions to seek judicial review of such actions. The Freedom of Information Act allows persons to utilize administrative and judicial remedies to seek government records. The Judicial Redress Act, which was enacted into law in 2016, provides EU citizens and citizens of other designated countries with the right to seek redress in U.S. courts if personal data shared with U.S. authorities by their home countries for law enforcement purposes is subsequently wrongfully disclosed. Citizens would also have rights concerning access and rectification of data, but only to the same extent as U.S. persons, subject to the same exemptions and exceptions. Once implemented, the United States anticipates that the Judicial Redress Act would be the primary mechanism for EU citizens to seek judicial redress in connection with access/rectification under the Agreement, although other statutes still remain in effect.

In addition to the administrative options described above, an EU citizen or resident may seek judicial redress from an adverse administrative action by filing a complaint with a court in an appropriate venue.

47. **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 41, above.

ANNEX II A

Terrorist Finance Tracking Program

Recent Examples of Cases in which TFTP Information has been used for the Prevention, Investigation, Detection, or Prosecution of Terrorism or its Financing
March 2016

(U) **CONTEXT**

(U) The U.S. Treasury Department's Terrorist Finance Tracking Program (TFTP) is a vital counter-terrorism tool that has produced thousands of valuable financial leads to counter-terrorism authorities, including more than 2,300 TFTP reports (which may contain multiple TFTP leads) provided to European authorities and over 3,350 such reports shared globally during its 14-year history. During the review period, from 1 March 2014 through 31 December 2015, Treasury also provided 11,678 TFTP-derived leads to EU Member States and EUROPOL for use in their counter-terrorism investigations. TFTP data provide key information including account numbers, names, addresses, transaction amounts, dates, branch locations, and sometimes even bills of lading, all of which are of tremendous value for counter-terrorism analysts in identifying previously unknown terrorist operatives and financial supporters. The examples below highlight recent cases in which the TFTP has provided key leads, as well as the ways in which TFTP-derived information has helped to identify the financial support networks behind leading terrorist organizations currently under investigation by U.S. and European authorities. The following are concrete examples where TFTP-derived information has been used in U.S. and European counter-terrorism investigations.

(U) In all cases, the U.S. government shares TFTP-derived information and counter-terrorism leads with relevant governments, as appropriate.

(U) **RECENT VALUE EXAMPLES**

(U) The TFTP was used in the investigation of Cherif and Said Kouachi. In January 2015, the Kouachi brothers forced their way into the office building of Charlie Hebdo, a satirical magazine. In the building, they shot and killed several individuals. On their way out, they executed a police officer on the sidewalk. Al Qaida in the Arabian Peninsula claimed responsibility for the attack. TFTP-derived information provided authorities the financial activities of Cherif and Said Kouachi, including names, accounts, addresses, and dates and amounts of transactions. This information was also shared with EUROPOL and used in Member State investigations. In total, Treasury provided nearly 600 TFTP-derived leads to EUROPOL in response to requests related to the January 2015 attacks.

(U) The TFTP was used in the investigation of nine ISIL-inspired terrorists, who worked together to commit multiple attacks in Paris on November 13, 2015. Three teams comprised of three people per team executed six separate attacks, resulting in 130 deaths and more than 350 injuries. TFTP-derived information provided authorities the financial activities of these attackers, including names, accounts, addresses, and dates and amounts of transactions. This information was also shared with EUROPOL and used in Member State investigations. In total, Treasury provided more than 900 TFTP-derived leads in relation to these attacks to EUROPOL and other counterterrorism authorities.

(U) The TFTP was used in the investigation of experienced jihadist and recruiter Ahmed Laidouni. Laidouni is a veteran of the Bosnian war and in 1998 joined an Al Qaida training camp in Afghanistan. He was suspected to be in contact with terrorists arrested in the United Kingdom in 2002 who were preparing ricin attacks. In 2004, he was arrested in France and sentenced to seven years in prison for recruiting jihadists for Afghanistan. In 2012, he went to Syria to join the Al Nusrah Front. Over the course of the next two years, he traveled to Spain, France, Algeria, Libya, Tunisia, and was arrested in Morocco in 2014 on suspicion of recruiting fighters for the Al Nusrah Front. It is suspected that Laidouni may have known the Kouachi brothers (perpetrators of the January 2015 Charlie Hebdo terrorist attack), as they were photographed together in 2010. TFTP-derived information provided authorities the financial activities of Ahmed Laidouni, including names, accounts, addresses, and dates and amounts of transactions. This information was also shared with EUROPOL and used in Member State investigations.

(U) The TFTP was used in the investigation of Davide DeAngelis. DeAngelis was arrested in Luxembourg in 2014 and extradited to Spain for his involvement in recruiting fighters for Syria. DeAngelis was believed to be in Syria in 2012 and, following his return to Europe, worked with Mustafa Maya Amaya on funding and recruiting new jihadists to join the Islamic State in Iraq and the Levant (ISIL) in Syria and Al Qaida in the Lands of the Islamic Maghreb in Mali. De Angelis was also believed to be one of a number of facilitators distributed throughout Europe in support of the Amaya network. This network, which was dismantled by Spanish and Moroccan authorities in 2014, was believed to be the biggest group in Europe recruiting jihadists for Syria. TFTP-derived information provided authorities the financial activities of Davide De Angelis, including names, accounts, addresses, and dates and amounts of transactions. This information was also shared with EUROPOL and used in Member State investigations.

(U) The TFTP was used in the investigation of Rutilio Sermonti and his associates. Sermonti and 14 other individuals were arrested in Italy in 2014, while stockpiling weapons for attacks on magistrates, police, public transportation, and the Equitalia tax collection agency. These attacks were believed to be an attempt by the group to destabilize the country. Sermonti was a former member of the banned Ordine Nuovo (New Order) far right group that carried out a string of terror attacks in the 1970s and 1980s in an effort to restore the Fascist regime of wartime dictator Benito Mussolini. In recorded conversations, the group referred to AK-47 assault rifles as “toffees” and stated that “this is the moment to strike, but not blindly,” noting that “banks, prefectures, police stations, Equitalia offices with their employees inside need to be hit.” TFTP-derived information provided authorities the financial activities of Rutilio Sermonti and his associates, including names, accounts, addresses, and dates and amounts of transactions. This information was also shared with EUROPOL and used in Member State investigations.

(U) The TFTP was used in the investigation of Edin Tabakovic, Ramiz Ibrahimovic, and Alaudin Ibrahimovic. These individuals were arrested in Bosnia and Herzegovina in 2015 and were suspected of financing terrorist activities and attempting to travel to Syria to join ISIL. Ramiz Ibrahimovic is believed to have fought in Syria and returned to Bosnia and Herzegovina in 2013. TFTP-derived information provided authorities the financial activities of these individuals, including names, accounts, addresses, and dates and amounts of transactions. This information was also shared with EUROPOL and used in Member State investigations.

(U) The TFTP was used in the investigation of the jihadist recruitment ring called the Al Andalus Brigade. This network was dismantled by Spanish police in 2014 and was sending individuals from Spain and Morocco to fight with ISIL. This group was led by a former Guantanamo Bay prisoner and Afghanistan veteran, and had a high level of professionalism, radicalism, and experience. Individuals underwent intense indoctrination and high-intensity physical and weapons training. According to the Spanish Interior Ministry, this recruitment ring had connections with terrorist groups in France, Belgium, Morocco, Tunisia, Egypt, Turkey, and Syria. At the time of the arrests, the group had five jihadists ready to travel to Syria, and two individuals recruited by the group had already been killed fighting in Syria/Iraq. TFTP-derived information provided authorities the financial activities of these individuals, including names, accounts, addresses, and dates and amounts of transactions. This information was also shared with EUROPOL and used in Member State investigations.

(U) The TFTP was used in the investigation of Jean Louis Denis. Denis was arrested in Belgium in 2014 on suspicion of recruiting fighters for extremist activities in Syria. Denis was a supporter of Sharia4Belgium, which was designated as a terrorist organization in Belgian court in 2015. Along with three other individuals, Denis would distribute meals to the needy to recruit people to go to Syria. Prosecutors believe that in addition to recruiting fighters, Denis radicalized the individuals and was involved in the logistics for their departure for Syria. TFTP-derived information provided authorities the financial activities of Jean Louis Denis, including names, accounts, addresses, and dates and amounts of transactions. This information was also shared with EUROPOL and used in Member State investigations.

(U) The TFTP was used in the investigation of Mohammad Abdulazeez. Abdulazeez was a homegrown extremist who attacked two U.S. military sites in 2015, killing several U.S. military members. TFTP-derived information provided authorities the financial activities of Mohammad Abdulazeez, including names, accounts, addresses, and dates and amounts of transactions.

(U) **ADDITIONAL U.S. GOVERNMENT TFTP-RELATED VALUE EXAMPLES**

(U) ***Background***

(U) As a general practice, the U.S. National Counterterrorism Center (NCTC) integrates financial intelligence into its terrorism investigations. While NCTC benefits from multiple sources of financial intelligence, information derived from the TFTP has provided valuable information to NCTC counter-terrorism investigators. For example, NCTC used financial intelligence in 61 lead cables in 2015. These lead cables provided valuable information on terrorists affiliated with the following groups: Al Qaida, Al Qaida in the Arabian Peninsula (AQAP), Al Qaida in the Islamic Maghreb (AQIM), Al Nusrah Front, Al Shabaab, Hizballah, the Islamic State of Iraq and the Levant (ISIL), and Lashkar-e-Tayyiba. NCTC also relies on financial intelligence to investigate terrorist threats to large events such as the Olympic Games, including the upcoming 2016 Summer Games in Rio. Below are several recent examples of where financial intelligence, including TFTP-derived information, has provided value to NCTC investigations.

(U) ***NCTC TFTP-Related Value Examples***

I. **ISIL**

A. (U) Financial intelligence, including TFTP-derived information, has been used in the investigation of an ISIL facilitation network. Such financial research led investigators to the true identity of a Syria-based operational planner in charge of identifying operatives who would be able to travel through Europe and, from Europe, to potentially conduct attacks in the United States.

B. (U) Financial intelligence, including TFTP-derived information, has been used in the investigation of a Syria-based ISIL operational planner, who was in contact with several individuals in the United States via social media. Such financial research helped investigators to confirm the locations of individuals within the planner's network and to identify additional methods used by the group to move funds.

C. (U) Financial intelligence, including TFTP-derived information, has been used in the investigation of a Dubai-based ISIL recruiter. Such research into the recruiter provided investigators with insight into two other ISIL facilitation networks, based in the Philippines and India. TFTP-derived information provided investigators with information about the recruiter's financial activities, including additional phone numbers and the identities of previously-unknown associates.

D. (U) Financial intelligence, including TFTP-derived information, has been used in the investigation of an Iraq-based ISIL facilitation network. Such financial research provided investigators with unique information about the network's contact with ISIL personnel participating in the group's weapons development program.

II. **Al Qaida (AQ)**

A. (U) Financial intelligence, including TFTP-derived information, has been used in the investigation of an AQ facilitation network. Such financial research led to the true identity of a Syria-based AQ facilitator. In addition, the research helped build out the facilitator's network, identifying true names of individuals in Egypt, Kuwait, Qatar, Syria, Tunisia, and Turkey, as well as a U.S. visa holder. Financial intelligence, including TFTP-derived information, also provided investigators with previously-unknown information about suspected associates residing in Bulgaria, France, Italy, the Netherlands, Norway, Romania, and the United Kingdom.

III. **Al Qaida in the Arabian Peninsula (AQAP)**

A. (U) Financial intelligence, including TFTP-derived information, has been used in the investigation of U.S.-based associates of AQAP members. Such financial research provided investigators with information leading to the identification of previously unknown users of two Yemeni phone numbers of interest.

IV. **Al-Shabaab**

A. (U) Financial intelligence, including TFTP-derived information, has been used in the investigation of an Al-Shabaab external operations network. Such financial research provided

investigators with information leading to the identification of network members located in the United States.

B. (U) Financial intelligence, including TFTP-derived information, has been used in the investigation of senior Al-Shabaab members. Such financial research provided investigators with information leading to the identification of phones numbers tied to a facilitation network in Canada.

ANNEX III

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 – 3 February 2016				
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	-/-	-/-
Oct-12	11/10/2012	105	No	-/-	-/-
Nov-12	08/11/2012	107	No	-/-	-/-
Dec-12	06/12/2012	109	No	-/-	-/-
Jan-13	09/01/2013	111	No	-/-	-/-
Feb-13	04/02/2013	115	No	-/-	-/-
Mar-13	06/03/2013	115	No	-/-	-/-
Apr-13 (1)	03/04/2013	119	No	-/-	-/-
Apr-13 (2)	22/04/2013	16	No	-/-	-/-
May-13	06/05/2013	124	No	-/-	-/-
Jun-13	05/06/2013	126	No	-/-	-/-
Jul-13	03/07/2013	127	No	-/-	-/-
Aug-13	06/08/2013	131	No	-/-	-/-
Sep-13	04/09/2013	133	No	-/-	-/-
Oct-13	30/09/2013	134	No	-/-	-/-
Nov-13	04/11/2013	137	No	-/-	-/-
Dec-13	04/12/2013	139	No	-/-	-/-

Jan-14	07/01/2014	142	No	-/-	-/-
Feb-14	05/02/2014	145	No	-/-	-/-
Mar-14	06/03/2014	147	No	-/-	-/-
Apr-14	08/04/2014	150	No	-/-	-/-
May-14	06/05/2014	153	No	-/-	-/-
Jun-14	03/06/2014	156	No	-/-	-/-
Jul-14	08/07/2014	160	No	-/-	-/-
Aug-14	05/08/2014	166	No	-/-	-/-
Sep-14	05/09/2014	170	No	-/-	-/-
Oct-14	07/10/2014	174	No	-/-	-/-
Nov-14	05/11/2014	177	No	-/-	-/-
Dec-14	03/12/2014	182	No	-/-	-/-
Jan-15	07/01/2015	182	No	-/-	-/-
Feb-15	02/02/2015	184	No	-/-	-/-
Mar-15	03/03/2015	187	No	-/-	-/-
Apr-15	09/04/2015	188	No	-/-	-/-
May-15	06/05/2015	189	No	-/-	-/-
Jun-15	02/06/2015	189	No	-/-	-/-
Jul-15	07/07/2015	186	No	-/-	-/-
Aug-15	05/08/2015	183	No	-/-	-/-
Sep-15	14/09/2015	175	No	-/-	-/-
Oct-15	30/09/2015	175	No	-/-	-/-
Nov-15	12/11/2015	173	No	-/-	-/-
Dec-15	08/12/2015	171	No	-/-	-/-
Jan-16	12/01/2016	169	No	-/-	-/-
Feb-16	02/02/2016	169	No	-/-	-/-
		120 Average (rounded)[14]			

[14] For the reporting period (March 2014 to December 2015): 174 (rounded)

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

Period	01 August 2010 – 3 February 2016		
Month	Communication with the Designated Provider		Total set of verification documentation (including DPO advice, verification decision)
	Delay notification[15]	Verification	Number of pages
Aug-10	06/08/2010	10/08/2010	+
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
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
Oct-12	-	12/10/2012	116
Nov-12	-	09/11/2012	117
Dec-12	07/12/2012	10/12/2012	117
Jan-13	-	11/01/2013	120
Feb-13	-	04/02/2013	123
Mar-13	-	08/03/2013	124
Apr-13 (1)	-	05/04/2013	128
Apr-13 (2)	-	22/04/2013	23
May-13	-	07/05/2013	133
Jun-13	-	07/06/2013	136
Jul-13	-	05/07/2013	136
Aug-13	-	07/08/2013	141
Sep-13	-	05/09/2013	143

[15] 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.

Oct-13	-	01/10/2013	144
Nov-13	-	05/11/2013	148
Dec-13	-	05/12/2013	150
Jan-14	-	07/01/2014	153
Feb-14	-	07/02/2014	157
Mar-14	-	07/03/2014	160
Apr-14	-	09/04/2014	162
May-14	-	08/05/2014	166
Jun-14	-	04/06/2014	169
Jul-14	-	09/07/2014	173
Aug-14	-	06/08/2014	178
Sep-14	-	05/09/2014	182
Oct-14	-	08/10/2014	187
Nov-14	-	06/11/2014	191
Dec-14	-	04/12/2014	195
Jan-15	-	07/01/2015	194
Feb-15	-	03/02/2015	197
Mar-15	-	04/03/2015	202
Apr-15	-	10/04/2015	204
May-15	-	08/05/2015	205
Jun-15	-	02/06/2015	207
Jul-15	-	09/07/2015	200
Aug-15	-	06/08/2015	198
Sep-15	-	16/09/2015	191
Oct-15	-	30/09/2015	191
Nov-15	-	12/11/2015	190
Dec-15	-	09/12/2015	187
Jan-16	-	13/01/2016	185
Feb-16	-	03/02/2016	185
			131 Average (rounded)[16]

[16] For the reporting period (March 2014 to December 2015): 188 (rounded)

C. Summary of monthly figures (as per 31 January 2016)

2010:

Month	08 2010	09 2010	10 2010	11 2010	12 2010
Article 4	1	1	1	1	1
Article 9[17]	6	1	1	0	0
Article 10[18]	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	10 2012	11 2012	12 2012
Article 4	1	1	1	1	1	1	1	1	1	1	1	1
Article 9	0	0	0	0	0	0	1	0	0	0	0	0
Article 10	4	6	2	1	3	7	4	6	0	4	7	3

2013:

Month	01 2013	02 2013	03 2013	04 2013	05 2013	06 2013	07 2013	08 2013	09 2013	10 2013	11 2013	12 2013
Article 4	1	1	1	2	1	1	1	1	1	1	1	1
Article 9	0	1	0	1	0	0	0	1	0	0	1	0
Article 10	5	2	5	1	7	7	7	2	5	3	5	2

2014:

Month	01 2014	02 2014	03 2014	04 2014	05 2014	06 2014	07 2014	08 2014	09 2014	10 2014	11 2014	12 2014
Article 4	1	1	1	1	1	1	1	1	1	1	1	1
Article 9	4	0	0	1	0	0	2	8	9	10	8	5
Article 10	9	3	3	9	5	5	10	1	2	7	7	3

2015:

Month	01 2015	02 2015	03 2015	04 2015	05 2015	06 2015	07 2015	08 2015	09 2015	10 2015	11 2015	12 2015
Article 4	1	1	1	1	1	1	1	1	1	1	1	1
Article 9	4	19	9	6	5	2	1	4	0	0	0	0
Article 10	18	8	9	7	6	11	18	9	15	8	24	9

[17] 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).

[18] 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).

2016:

Month	01 2016
Article 4	1
Article 9	0
Article 10	13

Overall:

03/2014 – 12/2015 (review period)	Sum
Article 4	22
Article 9	93
Article 10	194

Article 10 requests	
EU Member States (2014)	39
EU Member States (2015)	81

D. Summary of intelligence leads (as per 31 January 2016)

Article 9: Information spontaneously provided by the US	
Instances	**Leads**
119	2825
Article 10: Requests for searches	
Requests	**Leads**
394	13936

E. Use of TFTP in relation to Task Force Fraternité (Paris attacks)

Article 10: Requests for searches	
Requests	**Leads**
30	799

F. Use of TFTP in relation to the phenomenon of Foreign Fighters

Article 10: Requests for searches	
Requests	**Leads**
84	2771