EUROPEAN
COMMISSION

Brussels, 22.7.2019
SWD(2019) 301 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(2019) 342 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, an 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 fifth joint review of the Agreement since it entered into force and covers a period of thirty-five months between 1 January 2016 and 30 November 2018. 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]. The fourth joint review conducted in March 2016 covered a period of twenty-two months (1 March 2014 until 31 December 2015)[4]. 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[5].

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 (hereinafter "the Treasury"). The EU review team was headed by a senior Commission official and in total consisted of two members of Commission staff and representatives of two data protection authorities. A list of the members of both the EU and US review teams is included in Annex I to this Report.

The fifth joint review was carried out in two main steps: on 15 January 2019 in The Hague at Europol's premises and on 31 January and 1 February 2019 in Washington at 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. 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 asked further questions to Treasury officials on the spot 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.

---

1 SEC (2011) 438 final of 30.3.2011.
2 SWD (2012) 454 final of 14.12.2012.
3 COM (2014) 513 final and SWD (2014) 264 final of 11.8.2014.
4 COM (2017) 31 final and SWD (2017) 17 final of 19.1.2017.
5 COM (2013) 843 final of 27.11.2013.

– The review team members were granted access to the facilities of the TFTP overseers 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 a non-disclosure agreement as a condition for their participation in this review exercise.

– The review teams were given a demonstration of searches performed on the Provided Data, with the results shown and explained 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 General Counsel, 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 sent prior to the review, information obtained from the discussions with Treasury personnel and members of the U.S. review team, as well as information contained in other publicly available Treasury documents. In addition, the report takes into account information provided by Europol staff during the review, including submissions by Europol's Data Protection Officer. To complete the information available, the Commission also met and received information from the Designated Provider and organised a meeting on 3 April 2019 to receive feedback from Member States on the reciprocity provisions of the TFTP.

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 information at 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 fifth 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 EU overseer.

This report was prepared by, and reflects the views of, the EU review team, based on the work of the joint review and other work independently conducted on the EU side. However, the modalities for the fifth 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.

Finally, the recommendations expressed in this report do not necessarily reflect the personal views of individual members of the EU 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 [6]. This 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 and fourth 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

---

6 COM(2013) 843 final of 27.11.2013.

planning and financing. The TFTP helps to identify and track terrorists and their support networks.

In addition to the examples provided during the past four reviews and in the Joint Value Report, 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 in the EU and beyond in which TFTP information played a decisive or important role.

The review shows efforts 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 despite the limitations given by the nature of highly sensitive counter-terrorism investigations.

During the current review period, the EU has continued to significantly benefit more from the TFTP. It has become an increasingly important tool with the increase in the number of terrorist attacks since 2015. In some cases, the information provided under the Agreement has been instrumental in bringing forward specific investigations relating to terrorist attacks on EU soil.

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 a key and efficient instrument to provide timely, accurate and reliable information about activities associated with suspected acts of terrorist planning and financing. It helps to identify and track terrorists and their support networks worldwide.

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 and 192 such requests during the twenty-two months covered by the fourth review. Under the current review covering thirty-five months, the Treasury received 402 such requests. Europol has initiated in the current review period 32 requests and transmitted 374 requests from Member States.[7] There were 2 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 70,991 leads contained in the 292[8] responses provided to Member States and Europol as compared to 8,998 leads contained in the 121 responses provided to Member States and Europol during the period of the fourth 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 Stockholm on 7 April 2017, Barcelona on 17 August 2017 and Turku on 18 August 2017.

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.

Europol highlighted that, since the European Counter Terrorism Centre (ECTC) took up its activities in January 2016, information sharing and operational support provided by Europol to EU Member States and cooperation partners reached an all-time peak at the end of 2018, which also positively affected cooperation in the context of the TFTP. By the end of 2018, more than 95% of the intelligence leads (out of over 94,000 leads in total since the EU-US TFTP Agreement entered into force in 2010) were generated through the TFTP as of January

---

7 The total number of requests sent by Europol during this review period is slightly higher 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 402 requests received from Member States and the EU during the review period. Of these requests, 110 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 402 requests, some of the responses were provided to Europol after the conclusion of the review period.

2015 onwards, when EU counter terrorism efforts were boosted after the Charlie Hebdo attacks. Europol also submitted that the TFTP is, with the establishment of the ECTC, now made use of in every terrorist incident in which Europol is involved in information exchange or operational support activities as it is considered an instrumental contribution to support common counter terrorism efforts.

Pursuant to Article 9, the U.S. supplied 57 TFTP-derived reports consisting of 11,361 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 fourth 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. It is nevertheless clear that EU Member States' authorities would be able to process TFTP leads more efficiently if they were provided in a digital format. The Treasury submitted that this is not possible under the current arrangements relating to the security and integrity of the TFTP. The Commission invites the Treasury and Europol to continue considering ways to improve this situation.

The Commission proposes that Member States consider providing regular feedback, through Europol, on the added value of the TFTP leads 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 targeted 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 39,020 searches of the TFTP, for an average of 1,115 searches per month as compared to 1,232 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 35 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.

In addition to information received both orally and in writing from the Treasury and Europol, the review team examined, by way of representative sampling, three Article 4 requests' classified supporting documentation, including the verification documents prepared by Europol. On that basis, the review team discussed with the Treasury and Europol the procedures for the preparation and handling of their requests and scope.

The requests under Article 4 were received every month, and covered a period of four weeks. During the period under review, Europol received 35 requests from the Treasury. With an average duration of two days to perform its verification, The EU review team considers that Europol verifies requests made by the U.S. "as a matter of urgency" as required by Article 4(4) of the Agreement. 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, 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.

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.

Europol outlined its well-established verification process under Article 4 of the Agreement to the review team, which also includes a formal legal procedural review and obtaining advice from the Data Protection Officer of Europol for each request. The assessment of operational considerations, including security, 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, for each request, several internal actors (including a formal legal procedural review, advice from the Data Protection Officer and an operational assessment, prior to the authorisation of a request in each case). 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 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.

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. An analysis of the extracted data is conducted every year, analysing on a 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 Treasury conducted three such evaluations during the review period, covering the years 2015, 2016, and 2017, respectively. These annual evaluations each concluded 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 2018 evaluation had not been concluded by the end of the joint review period.

The EU review team suggests that the annual audit performed by the Treasury to ensure compliance with Article 4(2)(c) of the Agreement should be set up in a more quantitative manner, in particular by determining the message types and geographic regions that are the most and least responsive to TFTP searches. Message types and geographic regions that have been the least responsive could be 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. The outcome of such assessment should be included and taken into account in subsequent Article 4 requests.

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 was explained how a search at the Treasury takes place. 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 that 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 the overseers appointed by the Designated Provider and the EU. 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 overseer 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 39,020 searches conducted by the analysts, queried 645 searches and blocked 53 searches, the search terms of which were considered to be too broad. The Treasury analysts conducting searches could receive further training to narrow the scope of searches, prior to taking up their duties. This would likely have a positive effect on the number of blocked searches in the future.

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. For a portion of the review period, real time review was provided only by the overseer appointed by the Designated Provider, as the overseer appointed by the EU had not yet received all appropriate security clearances. When the EU-appointed overseer received the necessary security clearances, he conducted retrospective review of searches performed during the period when he did not have complete, full access to the search requests as well as recommencing his own

real time review of searches in addition to the review performed by the Designated Provider's overseer.

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 Treasury explained the technical safeguards and physical controls of the TFTP. 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 EU review team had the opportunity to speak to a representative of the Designated Provider responsible for auditing procedures to test data security and integrity 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 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.

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 deletes data on a rolling 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 30 November 2013 had already been deleted at the time of the review, well ahead of the due date, with the exception relating to an incident described below.

The Treasury informed the EU review team, both orally during the visit to Washington D.C. as well as in written response to the questionnaire in Annex IIA, about an incident that led to the retention of data beyond the time-period of five years as set by Article 6(4) of the Agreement.

The EU review team understands that in May 2017, several batches of data were inserted into new hardware. Long upload times suggested that this hardware was not capable of processing such data and therefore, the data was inserted into faster tier hardware. When this process was completed later that month, it was inadvertently omitted to delete the data on the initial new hardware.

The incident was uncovered in October 2018 and reported by the Treasury to the independent auditors contracted by the Designated Provider. Subsequently, the pertinent data on that hardware was swiftly removed, after it had been established that analysts had not accessed the data. The Treasury explained that such an incident will not be able to happen again, as the Treasury has amended its processes to ensure old data is removed if/when data is transitioned between storage areas, and the monitoring capabilities of the auditors has been extended to ensure they would detect such incidents in the future. In light of these explanations, confirmed by the independent auditors contracted by the Designated Provider, the EU review team is reassured that this was a one-time incident. The EU review team also took note of the circumstance that none of the data retained beyond the time-period was available for searching by Treasury analysts. As a result, the data has therefore not been accessed or disseminated.

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 of five years specified in Article 6 (4) to ensure that they continue to be retained 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 3.4. 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 third 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. During the fourth joint review, the Treasury informed the EU 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.

Procedures and mechanisms to review the necessity of the retention of extracted data are in place. In the course of the current review, no extracted data has been identified as requiring deletion. In fact, the EU review team considers that when judicial proceedings have been finally disposed of, Article 6 (7) demands that the data is deleted from the TFTP database. In this context, the Commission also encourages Member States to inform Europol and the Treasury of the follow up of cases regarding which it has received leads from the TFTP.

During the current review, the Treasury submitted that leads provided in the context of a case that is finally disposed of, could still be useful to uncover further links to terrorist networks and their financers in future investigations. The EU review team is not convinced that Article 6(7) of the Agreement allows for such extended use. Moreover, the EU review team also came across a case relating to a person, which has been disposed of years ago and who clearly had acted on its own. Data relevant to this case was nevertheless still retained in the TFTP database during the current review.

In the opinion of the EU review team, the issue of the retention of extracted data is exacerbated by the previously explained circumstance in section 3.3, that the overwhelming majority of messages accessed is actually never disseminated; most search results are viewed for a few seconds to determine their value and then closed, with no further action or dissemination. Since these messages are considered as "extracted data", they also fall within the scope of Article 6 (7) of the Agreement. The EU review team did not receive any assurance that this data is deleted at one point in time.

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. However, the Commission suggests that the Treasury improves its mechanisms to review the necessity of retaining so-called "extracted data" to ensure that this data is only retained for as long as necessary for the specific investigation or prosecution for which they are used (Article 6, par. 7). When a case has been finally disposed of, the Commission considers this should in principle lead to the deletion of extracted data relating to that case.

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 January 2019.

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.

The Commission and the Treasury worked together and in cooperation with the EU's (former) 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 previous review period, the Treasury identified and shared with the Commission certain refinements to the procedures that may facilitate the prompt receipt of requests from the NDPAs by the Treasury. The EU review team is not aware of any issues relating to the prompt receipt of requests from NDPAs during the current review period.

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. The review team also 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 the TFTP.

Nevertheless, the review team considers that there may be instances, where such information could be provided. In particular, in cases where the TFTP was publically reported to be used, there does not appear to be any reasonable legal limitation to safeguard the prevention, detection, investigation, or prosecution of criminal offences or to protect public or national security that would prevent such disclosure in line with Article 15 (2).

During the review period, the Treasury received one perfected request through a European NDPA, wherein an individual sought to exercise the provisions described in Article 15 of the Agreement. The Treasury Department responded to the European NDPA, confirming that the requester’s data protection rights were respected in compliance with the TFTP Agreement.

The Treasury explained to the review team the process and the technical aspects of preparing a responsible and correct response to a request. During the process monitored, 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 has the impression that the verification process performed by the responsible personnel in the Treasury under Article 15 has not included an independent

review of the condition in Article 5 (5) of the Agreement that searches shall be based upon 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.

The Commission notes that the procedures to process requests from persons whether their data protection rights have been respected in compliance with the Agreement appear to function efficiently. However, the Commission suggests that the Treasury ensure that such verifications should review the justification for the relevant searches.

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.

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 utilise 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 so-called 'Judicial Redress Act of 2015',–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 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 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.

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.

The review shows efforts 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 clearly explain 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 Treasury, in its annual evaluation of Article 4 Requests, assesses the message types and geographic regions that are the most and least responsive to TFTP searches. The outcome of such an assessment should be included and taken into account in subsequent Article 4 requests. This could result in a more narrowly tailored request to minimise the amount of data requested from the designated provider, in line with Article 4(2).

The Commission further suggests that the Treasury should improve its mechanisms to review the necessity of retaining so-called "extracted data" to ensure that this data is only retained for as long as necessary for the specific investigation or prosecution for which they are used (Article 6, par. 7). In this context, the Commission also requests Member States to inform

Europol as a Single Point of Contact (SPoC) for subsequent information of the Treasury when a case has been finally disposed of, which should in principle lead to the deletion of extracted data relating to that case. Particular attention should also be provided to extracted data that is viewed by the Treasury analysts but not disseminated further in the context of a specific investigation.

The Commission suggests that the Member States consider providing regular feedback to Europol, for onward sharing with the Treasury as appropriate, on the added value of the TFTP leads 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 targeted Article 10 requests. EU authorities submitted that the leads provided on paper by the Treasury could be more efficiently processed if they are provided digitally. The Commission invites the Treasury and Europol to consider ways to facilitate the processing of leads, in compatibility with the security arrangements of the TFTP. The Commission notes that the procedures to process requests from persons whether their data protection rights have been respected in compliance with the Agreement appear to function efficiently. However, the Commission suggests that the Treasury ensures that such verifications should cover all relevant rights under the Agreement, including that data has only been searched where there is 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.

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 2021.

Annex I – Composition of the review teams

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

- Mr. Laurent Muschel, Director, Security, Directorate-General Migration and Home Affairs, European Commission, Head of the EU review team
- Mr. Jeroen Blomsma, Policy Officer, Terrorism and Radicalisation, Directorate-General Migration and Home Affairs, European Commission
- Ms. Ines Walburg, expert on data protection, the Hessian Commissioner for Data Protection and Freedom of Information, Germany
- Mr. Ronny Saelens, Commissioner-Investigator, Data Protection Authority of the Police Information, Belgium

It is noted that Ines Walburg and Ronny Saelens 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:

– Ms. Lisa Palluconi, Associate Director, Office of Foreign Assets Control, U.S. Department of the Treasury (Head of U.S. delegation)

– Mr. Greg Gatjanis, Associate Director, Office of Foreign Assets Control U.S. Department of the Treasury

– Mr. Jacob Thiessen, Senior Counsel, Office of the General Counsel, U.S. Department of the Treasury

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

– Mr. Dylan Cors, International Director, National Security Division, U.S. Department of Justice

– Mr. Kenneth Harris, Senior Counsel for the European Union and International Criminal Law Matters, U.S. Department of Justice, U.S. Mission to the European Union

– Mr. Thomas Burrows, Associate Director for Europe and Senior Counsel for Multilateral Matters, Office of International Affairs, U.S. Department of Justice.

Annex II – Responses by the US Treasury Department to the EU questionnaire

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 covered the period from 1 March 2014 to 31 December 2015. The fifth review covers the period from 1 January 2016 to 30 November 2018.

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

a) the number of financial payment messages accessed;

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

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

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

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

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

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

II. Statistical information

1. In comparison to the period covered by the first four 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 35-month period between 1 January 2016 and 30 November 2018 (“the review period”). The increase is primarily the result of an increase in the volume of the message types responsive to the requests subject to the Agreement (each a “Request”) 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 review period, TFTP analysts conducted 39,020 searches of data provided by the Designated Provider, for an average of 1,115 searches per month. This number includes searches of financial payment messages sent by financial institutions around the world.

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 are not disseminated; most are 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 US authorities (substantially/slightly higher/lower, about the same)?

The provision of TFTP-derived information to EU and third-country authorities has increased substantially during the review period, due to terrorist attacks in Europe through 2018 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 has provided TFTP-derived information to competent U.S. authorities in connection with ongoing U.S. counter-terrorism investigations at about the same rate as in the prior review period.

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 review period, U.S. investigators supplied 459 TFTP-derived reports consisting of 11,361 leads pursuant to Article 9, and an additional 70,911 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, one Article 9 spontaneous report provided to Europol during the review period contained 525 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.

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.

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

U.S. investigators supplied 91 reports comprised of TFTP data to competent authorities of third countries during the 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 3,800 such reports have been provided to competent authorities throughout the world since the program began, the majority of which (more than 2,750 such reports, plus an additional 70, 911 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 citizens or residents of EU Member States "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, 91 reports consisting of TFTP-derived information was provided to third countries. When that information involved citizens or residents of a Member State, the provision of that information was pursuant to existing information sharing protocols, under which the Treasury Department committed to (1) evaluate all such information for its relevance and utility to the investigation, prevention, combating or prosecution of terrorism or its financing in the Member State, and (2) disclose that information to competent authorities of the Member State in the most expedient manner if relevant and useful.

In the event information cannot 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, the Third Joint Review in April 2014, and the Fourth Review in March 2016. Other sensitive, non-public or public TFTP- derived information was shown to officials from certain EU institutions having oversight responsibilities, such as officials of the European Commission 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 US Treasury's experience with receiving follow-on information conveyed back by Member States, Europol or Eurojust?**

During the review period, 57 reports consisting of 11,361 TFTP leads were provided to EU Member States and Europol as the spontaneous provision of information pursuant to Article 9.

The Treasury Department received positive feedback from Europol and certain EU Member States about the value of the Treasury Department’s provision of TFTP-derived information and its significant impact on European counterterrorist investigations. 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 appreciates 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 valuable information to EU authorities.

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 US Treasury Department on that information coming from EU-MS or Agencies?**

The Treasury Department received 402 requests from EU Member States and Europol pursuant to Article 10 during the review period and responded to all requests. TFTP searches resulted in the transmission of leads to the EU in response to 292 of the 402 requests. There were 70,911 leads contained in the 292 Article 10 responses provided to EU Member States and Europol during the review period. In October 2018 Europol provided the Treasury Department with

EU Member States' feedback regarding TFTP information that provided significant leads to European CT investigations via 19 Article 10 responses.

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 been, is, and intends to remain in full compliance with all of its commitments under the TFTP Agreement.

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 such issues have been identified.

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 has submitted its Article 4 Requests on a monthly basis. There have been no irregularities in the reporting since January 2016.

The Article 4 Requests initially 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 regularly performs a review of the extracted data received and the utility and necessity of the data for counter-terrorism purposes. The review is a quantitative and qualitative analysis that determines 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. In tandem with this regular review, the Treasury Department conducts a comprehensive annual evaluation of its Article 4 Requests to assess compliance with Article 4(2)(c). During the review period, the Treasury Department completed three annual evaluations, covering the years 2015, 2016, and 2017, respectively. These annual evaluations each concluded that the Requests were necessary for the purpose of

the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. As a result of these evaluations, the Treasury Department made certain streamlining adjustments that resulted in a more tailored Request containing the most recent and relevant data. The Treasury Department will be conducting its annual evaluation covering 2018 during the first quarter of 2019.

The Treasury Department will continue to review its processes and procedures for assembling Requests, for the purpose of ensuring 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 review period, Europol did not request supplemental information beyond that already being supplied by the Treasury Department with respect to Requests submitted pursuant to Article 4(1).

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 addition, in an ongoing effort to enhance the Requests beyond the requirements set out in Article 4(2), Europol officials have regularly provided comments aimed at making the Requests easier to review and verify, including suggestions for additional information, condensation of repetitious or formulaic language, and typographical and display corrections to improve the clarity and focus of the Requests. The Treasury Department has carefully considered these suggestions and generally adopted them.

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?

Please see response to question 11. 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.

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 fulfil 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.

Similarly, 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, which can include the TFTP, and Treasury Department officials periodically brief the Committees on these issues.

Finally, the Privacy and Civil Liberties Oversight Board is an independent agency within the Executive Branch of the U.S. Government. The Board is authorized to continually review the implementation of executive branch policies, procedures, regulations, and information sharing practices relating to efforts to protect the nation from terrorism, in order to ensure that privacy and civil liberties are protected. As a counterterrorism program, TFTP is subject to the Board's oversight authority. How the Board independently elects to exercise its oversight authorities with respect to TFTP is, of course, up to the Board.

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 ("DASPTR") 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 Treasury DASPTR also reviews administrative appeals, where applicable, from the Treasury Privacy Officer's Article 15 and 16 request determinations. 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,[1] along with the Inspector General of the Treasury Department, have oversight with respect to the entire 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))?

Treasury has not identified any new issues during the reporting period. Prior to the 2016 Joint Review, 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. This delegation made it possible to verify requester's identity without sending additional personal data to the United States. This authorized 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

[1] 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.

ensure the identity of requesters and reduce the risk of unauthorized disclosures of personal data.

During the 2014-2016 review period, the Treasury Department identified and shared with the Commission certain refinements to the procedures that have facilitated the Treasury's prompt receipt of requests from the NDPAs. These procedural modifications have improved the processing of Article 15 and 16 requests under the agreement. 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 40, and 41 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 that 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; the system automatically aborts searches that could potentially return with over 10,000 leads;

- Independent overseers retained by the Designated Provider and the European Commission with appropriate U.S. Government national security clearances 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. With the transition to a newly updated system, technical system controls further solidified. In particular in response to the audit incident described in response to Question 30, the Treasury Department enhanced the Auditors monitoring capabilities as well as the scope of the automated data deletion process

25. What is the policy for log files (which data processing activities are logged, who have 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 on-going and at least annual evaluation to identify non-extracted data that are no longer necessary to combat terrorism or its financing changed since the last Joint Review (Article 6(1))? If so, what changes have occurred? Have such data been promptly and permanently deleted since the last Joint Review?

No measures to identify unnecessary non-extracted data have changed since the last Joint Review. Treasury does not retain any non-extracted information that is not responsive to the current 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 30 November 2013 been deleted as provided for in Article 6(4) of the Agreement?

Yes. However, we note one audit incident in which some non-extracted data was held on the system past the time period even though it was not available for searching by analysts. On 4 October 2018, the Department of the Treasury alerted the source's contract auditors that a database containing 11 deliveries covering July 2012 through September 2013 was inadvertently retained following the transition of data to a new storage area. The incident began when, on 8 May 2017, the data from 11 deliveries was moved to faster tier hardware for ingestion to the system. The re-ingestion of the data to the new hardware completed on 22 May 2017, but the deletion of the data on the old hardware didn't happen. The auditors confirmed that the out of scope data was last accessed or modified on 8 May 2017 and no personnel accessed the data since that time. This was a one-time issue and not a deficiency in our processes or tools. We will amend our processes to ensure old data is removed if/when data is transitioned between storage areas, and we are in discussions with the auditors to add additional capability to the automated process. Other than this incident, all non-extracted data received prior to 31 January 2014 was deleted in accordance with Article 6(4) of the Agreement.

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

The Treasury Department continues to assess these data retention periods as part of its regular review, analysis, and audit of data, as described in response to Question 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 fifth 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 Questions 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 regular assessments to ensure that any non-extracted data received on or after 31 January 2014 are deleted five years from receipt. This process is conducted in a way that ensures the system remains fully operational and all safeguards remain in place. All non-extracted data received prior to 31 January 2014 has been deleted. See Question 30 for additional information on process improvements to ensure old data is removed if or when such data is transitioned between storage areas.

34. 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.

35. Please describe how requests for subsequent dissemination of original TFTP- derived information are handled. Have any of these requests been rejected?

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

Yes. At all times during the review period, searches run on TFTP data were subject to real time and retrospective review. For a portion of the review period, real time review was provided only by the overseer appointed by the Designated Provider, as the overseer appointed by the EU had not yet received all appropriate security clearances. When the EU-appointed overseer received the necessary security clearances, he conducted retrospective review of searches performed during the period when he did not have complete, full access to the search requests as well as recommencing his own real time review of searches in addition to the review performed by the Designated Provider's overseer.

37. 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 – one appointed by the European Commission and the others employed by the Designated Provider – routinely request additional information to ascertain strict adherence to the counterterrorism 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 645 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 stopped 75 searches at the time of the search and, of all searches queried, blocked 53 searches during their retrospective review of the search logs because they believed the search terms were too broad. Stopped searches accounted for a small number of cases (75 total searches during the 35 months of the review period – or 0.19 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 645 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.

38. 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 (53 searches during the review period – or 0.19 percent), the overseers blocked the searches because they believed the search terms were too broad. In some cases, however, the search terms were only found to be overbroad because of a typographical error in the spelling of a terrorism suspect's name, or the inadvertent 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.

39. 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.

40. 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?

The Treasury Department received one perfected Article 15 request from a European NDPA during the current review period. The Treasury Department provided a response to the European NDPA and the decision was upheld on administrative appeal. 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.

Administrative redress under U.S. law consists of the right to an administrative appeal of an initial decision in response to a request under Article 15 or 16. The United States has agreed that the Treasury Department shall treat all persons equally in the application of its administrative redress process, regardless of nationality or country of residence. On November 27, 2017, the Treasury DASPTR issued a decision on the first administrative appeal Treasury has received under the TFTP agreement. In this decision, the DASPTR upheld the Treasury Privacy Act Officer's decision under Article 15. He also advised the requester of his right to appeal the decision by filing suit in the United States District Court for the District of Columbia and explained in more detail than the Privacy Officer had used in the letter communicating the initial decision that gave rise to the appeal why additional information beyond a statement that the requester's rights were respected under the agreement could not be provided.

Judicial redress under U.S. law would consist of the right to seek redress in federal court 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 generally to seek

judicial review of such actions. The Freedom of Information Act allows persons to utilize administrative and judicial remedies to seek government records, subject to specific exceptions. The Judicial Redress Act, which was enacted into law in 2016, provides EU citizens and citizens of other designated countries the right to seek redress in U.S. courts if they are wrongfully denied access to personal data that their home countries have shared with certain U.S. authorities (including the relevant elements of the Treasury Department) for law enforcement purposes, wrongfully denied the ability to rectify such data, or if such information is knowingly, wrongfully disclosed.

The Treasury Department received no requests pursuant to Article 16 of the TFTP Agreement during the review period.

As of December 31, 2018, the Treasury Department has no perfected requests pending pursuant to Articles 15 or 16 of the TFTP Agreement.

41. 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?

Since the 2016 Joint Review, Treasury received one perfected request pursuant to Article 15 of the TFTP Agreement. The Treasury Department confirmed that the requester's data protection rights were respected in compliance with the TFTP Agreement and explained why additional information could not be provided.

42. 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 inaccurate data was received or transmitted pursuant to the Agreement.

43. 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.

44. 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.

45. 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?

Yes. See the answer to question 40 above.

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

Annex IIA – Examples of cases in which TFTP has been used

Examples of Cases 2016-2018 in which TFTP Information has been used for the Prevention, Investigation, Detection, or Prosecution of Terrorism or its Financing
January 2019

The Terrorist Finance Tracking Program (TFTP) is a vital counter-terrorism tool that in its 17 year history has produced nearly one hundred thousand leads to counter-terrorism authorities world-wide. TFTP data provides key information, including account numbers, names, addresses, transaction amounts, dates, branch locations, and occasionally bills of lading, that are of tremendous value to counter-terrorism analysts in identifying previously unknown terrorist operatives and financial supporters. The examples below highlight cases in which TFTP provided key leads, as well as the various methods in which TFTP-derived data may have helped to identify the financial support networks behind leading terrorist organizations currently under investigation by U.S. and European authorities.

2016

- TFTP was used in the investigation of Mohamed Belkaid. Belkaid was an associate of Salah Abdeslam and is believed to have been active in the November 2015 Paris attack. He was killed in a shoot-out with Belgian police March 15, 2016. It is suspected that Belkaid may have been part of a plan for a Paris-style shooting attack at the same time of the Brussels bombing. TFTP-derived information provided authorities the financial activities of Mohamed Belkaid, which included names, accounts, addresses, dates and amounts of transactions. This information was also shared with Europol and used in EU member state investigations.

- TFTP was used in the investigation of Djamal Eddine Ouali. Ouali was detained in Italy on a European arrest warrant and extradited to Belgium. It is believed Ouali was involved with a network that produced forged documents used by terrorists in the March 2016 Brussels and November 2015 Paris attacks. TFTP-derived information provided authorities the financial activities of Djamal Eddine Ouali, which included names, accounts, addresses, dates and amounts of transactions. This information was also shared with Europol and used in EU member state investigations.

- TFTP was used in the investigation of Anis Bahri. Bahri was arrested in the Netherlands and was suspected of planning a terrorist attack for ISIL along with Reda Kriket. When arrested, Bahri had approximately 100 pounds of ammunition and an AK-47 assault rifle. TFTP derived information provided authorities the financial activities of Anis Bahri, which included names, accounts, addresses, dates and amounts of transactions. This information was also shared with Europol and used in EU member state investigations. We understand that Bahri was extradited to France in May 2016.

- TFTP was used in the investigation of Milazim Haxhiaj, Besnik Latifi, Enis Latifi, and Gazmend Haliti. These individuals were arrested by Kosovo police and convicted of planning terrorist acts. The four were arrested while planning to publish allegiance to ISIL on the internet to prove the group was expanding into the Republic of Kosovo. When arrested, there was suspicion that the group intended to poison a lake that is a source of water for residents in Pristina; however, Kosovo authorities later dropped that charge. TFTP-derived information provided authorities the financial activities of Milazim Haxhiaj, Besnik Latifi, Enis Latifi, and Gazmend Haliti, which included names, accounts, addresses, dates and amounts of transactions. This information was also shared with Europol and used in the investigation.

- TFTP was used in the investigation of Mohamed Amine Aissaoui. Aissaoui was arrested in Istanbul, Turkey on an international warrant for terrorism issued by the Spanish National Police. Investigators believe Aissaoui had been fighting with ISIL in Syria and was returning to Europe. Police are investigating whether his return was the result of plans to attack an EU country or if he had deserted ISIL. TFTP-derived information provided authorities the financial activities of Mohamed Amine Aissaoui, which included names, accounts, addresses, dates and amounts of transactions. This information was also shared with Europol and used in EU member state investigations.

- TFTP was used in the investigation of the Sunnah Association. Sunnah was believed to be supporting terrorist groups in Syria with supplies, to include decommissioned ambulances from Germany. It is a common practice in the Syrian conflict to transport fighters in ambulances in combat zones. TFTP-derived information provided authorities the financial activities of the Sunnah Association, which included names, accounts, addresses, dates and amounts of transactions. This information was also shared with Europol and used in EU member state investigations.

2017

- On 7 April 2017, Rakmat Akilov deliberately drove his hijacked truck into crowds of people along Drottninggatan in Stockholm, Sweden. On 10 April 2017, Europol submitted an urgent Article 10 request on behalf of Belgium to the U.S. Department of the Treasury to identify potential leads connected to Akilov. Treasury responded with twelve leads within five hours. The next day Europol requested release of the response to Poland due to a Polish connection to the investigation. Treasury approved the release within two hours.

- On 20 April 2017, Karim Cheurfi, wielding an AK-47 rifle on the Champs-Elysees in Paris, attacked French National Police Officers. French police killed Cheurfi after the exchange. On behalf of France, Europol submitted an urgent Article 10 request to the U.S. Department of the Treasury to identify potential leads in support of the French terrorism investigation. Treasury responded with two leads within three hours.

- On 17 August 2017, Younes Abouyaaqoub drove a van onto the pavement of Barcelona's La Rambla, ramming into pedestrians and cyclists. At about 1 a.m., 18 August, Houssaine Abouyaaqoub, Omar Hichamy, Moussa Oukabir, and Said Aalla were in a vehicle that drove into a crowd of pedestrians in Cambrils, Spain. After the car rolled over, the five individuals attacked bystanders with knives. A Spanish police officer killed all five assailants. Within a few hours Europol submitted an urgent Article 10 request to the U.S. Department of the Treasury on behalf of Spain. Thirty minutes later Europol provided additional information. Within two hours Treasury responded to Europol with 24 leads. The next morning Europol submitted a second Article 10 request for Spain and Treasury responded within four hours with seventeen leads. On Saturday morning 19 August, Europol indicated that six of the leads from the first Article 10 response were significant and requested Treasury approve Spain's use of the six leads for warrants. Europol also submitted a third Article 10 request in support of Spain's continuing investigation. Treasury approved the Europol request to use the leads to justify legal warrants.

- On 18 August 2017, Abderrahman Mechkah attacked people with a knife in Turku, Finland in a terror attack. Police shot Mechkah in the leg and arrested him. On 23 August 2017, Europol submitted a priority Article 10 request for Finland to the U.S. Department of the Treasury to potentially identify leads connected to the attack. Treasury responded with 563 leads on 25 August.

2018

- TFTP information was provided in support of a Slovakian counterterrorism investigation of five suspected terrorists and identified financial accounts/transactions for four of the five terrorists. The results provided over 500 leads of possibly some previously unreported associates/entities. The information proved valuable to Slovakia, as they are now considering criminal proceedings against some of these terrorists.

- Significant TFTP information was provided in support of an Italian investigation into suspected financing of terrorist groups in Libya via oil smuggling (from a North African country to Europe, via Malta and Italy). The searched selectors returned over 3200 leads that contained the financial accounts/transactions for many of the investigated persons and companies. The leads were critical to Italian authorities, who fully identified one of the main terrorist suspects with date of birth and identification document number information. The leads could eventually result in an international arrest warrant.

- TFTP information was provided in support of a Belgian investigation into individuals of North Caucasus origin (mainly Chechen), suspected of financing terrorism. The network is linked to several NGOs in Belgium, France, Germany, and Sweden whose activities are related to raising funds allegedly for charity. It is suspected that the funds are in fact being used to finance terrorist groups or individual Foreign Terrorist Fighters (FTF). The searched information returned more than 530 financial leads concerning some of the suspected FTFs and non-profit organizations. The TFTP leads provided significant value by generating relevant hits against Europol databases

that developed additional leads and helped map a complete financial picture of the main suspect. TFTP information was provided in support of an Italian investigation into terrorism finance by the terrorist group Al-Shabaab, which operates in several European countries. Al-Shabaab is primarily involved in facilitating clandestine immigration of Somali citizens through the provision of transportation, fake ID documents, and accommodation. Part of the proceeds of the migrants' smuggling is thought to be diverted to Al-Shabaab leading members. The searched information returned more than 410 financial leads. TFTP data revealed significant financial flows from one of the main suspects located in Malta to the United Kingdom and disclosed a possible further line of investigation.

U.S. Value Examples

2018

- TFTP research identified a large financial transfer that a U.S. terrorist initiated to a previously unknown terrorist.
- TFTP research identified financial transfers from several U.S. persons to a terrorist. Information was provided to law enforcement for monitoring.
- TFTP research on a known terrorist identified several transfers that a non-U.S. terrorist supporter made. At some point the supporter was in the U.S. for a conference; the information was provided to law enforcement for monitoring.

Annex III – Europol statistical information

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

Period	January 2016 – November 2018				
Month	Article 4 request		Communication with the Designated Provider		Total set of verification documentation (including DPO advice, verification decision)
	Date of receipt	Number of pages	Delay notification[9]	Verification	Number of pages
Jan-16	12/01/2016	169	-	13/01/2016	185
Feb-16	02/02/2016	169	-	03/02/2016	185
Mar-16	08/03/2016	169	-	10/03/2016	186
Apr-16	05/04/2016	167	-	06/04/2016	184
May-16	03/05/2016	170	-	04/05/2016	187
Jun-16	07/06/2016	166	-	08/06/2016	182
Jul-16	05/07/2016	160	-	08/07/2016	176
Aug-16	09/08/2016	153	-	10/08/2016	170
Sep-16	08/09/2016	152	-	09/09/2016	169
Oct-16	05/10/2016	152	-	06/10/2016	168
Nov-16	07/11/2016	152	-	09/11/2016	169
Dec-16	06/12/2016	154	-	07/12/2016	172
Jan-17	04/01/2017	155	-	05/01/2017	172
Feb-17	07/02/2017	157	-	08/02/2017	174
Mar-17	09/03/2017	148	-	10/02/2017	168
Apr-17	06/04/2017	149	-	07/04/2017	167
May-17	08/05/2017	151	-	11/05/2017	168
Jun-17	07/06/2017	152	-	09/06/2017	170
Jul-17	05/07/2017	153	-	07/07/2017	172
Aug-17	08/08/2017	146	-	10/08/2017	166
Sep-17	13/09/2017	148	-	14/09/2017	167
Oct-17	03/10/2017	150	-	04/10/2017	169
Nov-17	07/11/2017	152	-	09/11/2017	171
Dec-17	07/12/2017	158	-	08/12/2017	177
Jan-18	09/01/2018	194	-	11/01/2018	212
Feb-18	06/02/2018	132	-	08/02/2018	150

[9] 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.

Mar-18	06/03/2018	136	-	08/03/2018	155
Apr-18	03/04/2018	138	-	05/04/2018	157
May-18	07/05/2018	141	-	08/05/2018	160
Jun-18	05/06/2018	144	-	06/06/2018	162
Jul-18	03/07/2018	146	-	05/07/2018	164
Aug-18	10/08/2018	144	-	10/08/2018	165
Sep-18	11/09/2018	146	-	13/09/2018	167
Oct-18	09/10/2018	209	-	11/10/2018	231
Nov-18	13/11/2018	212	-	15/11/2018	234
		157 Average (rounded)			175 Average (rounded)

B. Summary of monthly figures (as per 1 January 2016)

2016

Month	01 2016	02 2016	03 2016	04 2016	05 2016	06 2016	07 2016	08 2016	09 2016	10 2016	11 2016	12 2016
Article 4	1	1	1	1	1	1	1	1	1	1	1	1
Article 9[10]	0	0	4	1	0	0	0	0	2	0	0	3
Article 10[11]	13	9	9	11	10	11	10	9	5	9	14	12

2017

Month	01 2017	02 2017	03 2017	04 2017	05 2017	06 2017	07 2017	08 2017	09 2017	10 2017	11 2017	12 2017
Article 4	1	1	1	1	1	1	1	1	1	1	1	1
Article 9	0	0	0	0	2	0	0	0	0	0	2	7
Article 10	16	15	8	7	8	15	3	19	11	12	8	10

2018

Month	01 2018	02 2018	03 2018	04 2018	05 2018	06 2018	07 2018	08 2018	09 2018	10 2018	11 2018
Article 4	1	1	1	1	1	1	1	1	1	1	1
Article 9	9	0	3	0	4	8	3	1	1	3	0
Article 10	10	17	10	18	10	11	13	12	15	23	15

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

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

C. Summary for the review period

01/2016 – 11/2018 (review period)	Sum
Article 4	35
Article 9	53
Article 10	408

Article 10 requests			
Requester	2016	2017	2018 (until 11/2018)
EU Member States	111	123	140
Europol	9	9	14
Eurojust	2	0	0
Total	122	132	154

D. Summary of intelligence leads (overall, as per 30 November 2018)

Article 9: Information spontaneously provided by the US	
Instances	**Leads**
172	10,519
Article 10: Requests for searches	
Requests	**Leads**
789	84,375

E. Use of TFTP in relation to the phenomenon of foreign fighters (overall, as per 30 November 2018)

Article 9: Requests for searches	
Requests	**Leads**
113	13,146
Article 10: Requests for searches	
Requests	**Leads**
247	34,432