EUROPEAN
COMMISSION

Brussels, 11.11.2022
SWD(2022) 357 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 PARLIAMANT 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(2022) 585 final}

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 Designated 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[1].

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."

[1] OJ L 195/5 of 27.7. 2010.

This report concerns the sixth joint review of the Agreement since it entered into force and covers a period between 1 December 2018 and 30 November 2021. The previous joint reviews of the Agreement were conducted in February 2011[2], in October 2012[3], in April[4], in March 2016[5] and in January 2019[6]. 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[7].

In line with Article 13 (3) of the Agreement, for the purposes of the review, the European Commission represented the European Union and the U.S. Treasury Department represented the United States. 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 sixth joint review was carried out in two main steps: on 8 March 2022 in The Hague at Europol's premises and on 29 and 30 March 2022 in Washington DC at the U.S. Treasury Department (hereinafter "the Treasury"). The following methodology was applied:

– Both review teams first met in The Hague at Europol's headquarters and were briefed by Europol senior staff and experts on Europol's implementation of the Agreement. Prior to the visit, Europol provided a written contribution to the review, including the relevant statistical information (Annex II).

– To prepare for 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 III). 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.

– All meetings were held in a dedicated meeting room, and as the review team largely consisted of the same members as during the fifth review, the Commission members of the EU review team agreed with the Treasury to use additional time to review documents and not revisit the facilities of the TFTP overseers in the Treasury or get a demonstration of searches performed on the Provided Data. For security reasons, review team members were required to sign a copy of a non-disclosure agreement as a condition of their participation in this review exercise.

2 SEC (2011) 438 final of 30.3.2011.
3 SWD (2012) 454 final of 14.12.2012.
4 COM (2014) 513 final and SWD (2014) 264 final of 11.8.2014.
5 COM (2017) 31 final and SWD (2017) 17 final of 19.1.2017.
6 COM(2019) 342 final, and SWD (2019) 301 final of 22.7.2019
7 COM (2013) 843 final of 27.11.2013.

– 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.

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 US 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 members of the EU review team also met and received information from the Designated Provider and organised a meeting on 24 January 2022 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 sixth 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 services would like to acknowledge the excellent cooperation on the part of all Treasury and other US 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 sixth review and the procedure for the issuance of this report were agreed with the Treasury, including an opportunity for the latter of prior reading of this report for the purpose of identifying any classified or sensitive information that could not be disclosed to the public.

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

3. THE OUTCOME OF THE JOINT REVIEW

3.1. The value of the TFTP Provided Data

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

Since the entry into force of the Agreement and in response to the Commission services' requests, the US 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[8]. 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 planning and financing. The TFTP helps to identify and track terrorists and their support networks. The fifth review provided 13 de-classified examples on how TFTP leads had been used in European investigations and three additional US value examples. Annex IV of this report provides for twelve additional examples on the use of TFTP data during the review period. The Treasury provided ten additional classified TFTP-derived value examples at the meeting with the review team in Washington DC on 29 and 30 March 2022.

In addition to the examples provided during the past five reviews, this review includes fourteen recent cases (listed in Annex IV), which 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.

[8] COM(2013) 843 final of 27.11.2013.

During the current review period, the EU has continued to significantly benefit more from the TFTP, and almost 50% of the leads resulting from all the searches go to Europol. 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 Member State authorities over the time, the Commission services are 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 US 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 such requests during the seventeen months covered by the third review, 192 requests during the twenty-two months covered by the fourth review and 402 requests covering during the thirty-five months covered by the fifth review. Under the current review, covering thirty-six months the Treasury received 508 such requests. Europol has initiated in the current review period 52 requests and transmitted 456 requests from Member States. There were no new requests by Eurojust covered by this review.

The number of leads generated by the TFTP in response to Article 10 requests has decreased since the last review. During the review period, there were 47 845 leads contained in the 262[9]

[9] The Treasury responded to all 508 requests received from Member States and the EU during the review period. Of these requests, 202 searches were returned without results, which is more than during the

responses provided to Member States and Europol as compared to 70 439 leads contained in the 292 responses provided to Member States and Europol during the period of the fifth review. However, the number of leads remains higher compared with the forth review, both in terms of the total number of leads and leads per request.

Annex IV 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 Vienna on February 2021 and made significant contributions to map out terrorist networks in a number of cases, often filling in missing links in an investigative chain.

Throughout the implementation of the Agreement, Europol played an active role in raising the awareness of the possibilities available under the TFTP by promoting the reciprocity provisions through the Liaison Bureaux at Europol and dedicated campaigns in Member States., 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 during the review period proactively initiated a series of requests under Article 10. The leads received were shared with relevant EU authorities to support investigations. This has helped raise awareness of added value of the TFTP, resulting in an increased use of the TFTP by those authorities.

Europol highlighted its role in European investigations of terrorist attacks and financing networks and its increasing role as an information hub since the European Counter Terrorism Centre (ECTC) took up its activities in January 2016. The average number of leads per month decreased from 2 232 to 1 631 during the review period, but remains at a high level during the review period. 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 US supplied 66 TFTP-derived reports consisting of 10 884 US leads during this review period, and 21 403 since the TFTP Agreement entered into force in 2010. 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 US 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

---

previous review period. 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 508 requests, some of the responses were provided to Europol after the conclusion of the review period.

general, and in line with what was submitted in the fifth joint review, the Treasury explained that the US 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 services invites the Treasury and Europol to continue to reflect on this possibility. The EU review team suggested that detailed written guidance should be given to TFTP users/analysts in relation to the handling of the extracted data contained in printed results of searches.

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 III 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 29 807 searches of the TFTP, for an average of 828 searches per month as compared to 1 115 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. .

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 36 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. It can be noted that the number of searches was reduced during the mandatory telework period in 2020 by a reduction of 54% from 2019 and 33% from 2021. This reduction in searches is also attributed to some residual impact resulting from reduced staffing due to the U.S. Treasury Department's COVID-19-related "mandatory telework" and "maximum telework" policies which remained in effect throughout the remainder of the review period.

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 US 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, two Article 4 requests' classified supporting documentation. Europol also provided additional written information on the workflows and processes relating to the Article 4 US requests to obtain data from the Designated Provider, which demonstrates efforts to improve transparency and accountability. 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, with the exemption of three months when mandatory telework applied at the Treasury[10] . During the period under review, Europol received 33 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 US "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 II.

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. Europol also informed the review teams of the EDPS TFTP Inspection[11] that took place on 5 to 6 February 2019, its findings, recommendations and Europol's follow-up actions, including the need to make changes in the Article 4 requests from one month another

[10] No Article 4 request were sent during the Treasury's "mandatory telework policy" period in April, May and July 2020 due to the covid-19 Pandemic.

[11] EDPS case number: 2018-0638

to more visible. The process for preparation, verification and validation of Article 4 requests by the Treasury remained the same as in the previous review. In addition, Europol explained that the TFTP Agreement does not stipulate a retention period for data included in the Article 4 requests and that this is regulated by the Europol Regulation. 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 Treasury's Office of Foreign Assets Control reviews the relevant documents and confirms that the Article 4 standards are satisfied and that the request reflects current counter-terrorism reports and analyses, while the Director of the Office of Foreign Assets Control provides final authorisation.

Article 4 requests take into account the results of the Treasury's regular evaluation of the extracted data received and the utility and necessity of the data for counter-terrorism purposes. A large-scale audit and analysis of the extracted data is conducted every year, analysing on a quantitative and qualitative basis the types of data most relevant to counter-terrorism investigations, and the geographic regions where the terrorist threat is particularly high or most relevant or susceptible to relevant terrorist activity.

The Treasury conducted two such large-scale evaluations during the review period. The 2018 annual evaluation was submitted on March 6, 2020, and the joint 2019-2020 evaluation on May 4, 2021. The Treasury Department made certain streamlining adjustments that resulted in a more tailored Request containing the most recent and relevant data. During the 2019-2020 evaluation, the Treasury recommended adding three jurisdictions to the requests to counter the threat posed by racially or ethnically motivated and violent extremists and removing three jurisdictions from the Requests that were of less value than others for purposes of prevention, investigation, detection, or prosecution of terrorism or its financing. It was also recommended to remove two messages types that provided leads of only limited utility. The Treasury Department will be conducting its annual evaluation covering January 2021 to December 2021 during the midyear of 2022, with final results expected prior to September 2022. This annual evaluation will assess the impact of the removal of some jurisdictions and whether circumstances justify their inclusion in the future.

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 services acknowledges the benefits of the close cooperation between the US authorities, Europol and EU counter-terrorism authorities in assessing and communicating on terrorism-related threats, and underlines the importance of that such cooperation to identify terrorism related threats, on which the requests are based, continues to remain distinct from Europol's verification role under Article 4 of the Agreement.

The EU review team received information from the Designated Provider on the security measures put in place in order to ensure the protection of Provided Data. The Designated Provider also confirmed that it had not encountered any issues in relation to the transfer of data under the Agreement. Together, they constitute an overall control framework, including for instance the role of the external security auditor and the Designated Provider scrutineers who oversee that the Provided Data are only used for the purpose of investigating terrorism financing and the monitoring of the deletion of data after a period of 5 years.

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

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.

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.

The EU review team welcomes the increased efforts to ensure that the annual audit and assessments performed by the Treasury to ensure compliance with Article 4 (2) of the Agreement are set up in both a quantitative manner, in particular by determining the message types and geographic regions that are the most and least responsive to TFTP searches and a qualitative manner, such as by identifying a recent threat or waning threats to focus on the most appropriate message types and geographic regions. Article 4 justifications for specified message type or geographic regions should be updated with more recent examples and continue to be legally justified in accordance with Article 4 (2). The EU review team encourages the Treasury to continue to scrutinise message types and geographic regions that have been the least responsive as part of their annual audit 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 EU review team welcomes these efforts that resulted in updates of the geographic scope and in a reduced number of message types being covered by production orders during the review period, and encourages the Treasury to continue such efforts and consider more frequent assessments, also in order to minimise the data requested and transferred. .

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 20 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 review team was explained how a search at the Treasury takes place. The analysts operating the searches explained 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 one of the three full-time overseers appointed by the Designated Provider and the overseer appointed by the European Commission. 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 EU review team was given access to all logs of individual TFTP searches made in the review period and made a random selection of 20 searches and their log files for a detailed review. Some information in the selected samples were considered classified due to ongoing investigations and could not be disclosed to the EU review team. The overseers confirmed that they had made full use of these powers: all overseers, including the overseer appointed by the European Commission, had requested additional information on an ongoing 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 29 807 searches conducted by the analysts, queried 697 searches and blocked 114 searches, the search terms of which were considered to be too broad. The Treasury analysts conducting searches are offered to receive further training to narrow the scope of searches, prior to taking up their duties or on an ad hoc basis.

The overseers verified the majority of the searches as they occurred and all of the searches, including those reviewed as they occurred, within one working day.

The overseers work in a complementary way by supporting each other in order to accomplish their tasks. The fact that a search has been selected for scrutiny by one of the overseers is visible to the other overseers, who would generally not select the same search in order to avoid the duplication and maximize the efficiency of the oversight. In 2013, the Commission and the Treasury agreed on measures further supporting the role of the EU overseer(s). The EU overseer(s) 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 COVID-19 pandemic did not materially affect the safeguards, controls, or reciprocity provisions set out in the Agreement. The role of overseers, auditors, and the supervision of security measures to safeguard classified information were not affected except in terms of adjusting staffing levels during the mandatory telework period in 2020. Live and retroactive review of system access and searches conducted on system were available and functioning during the period of review. The overseers' workspace experienced flooding during the current review period, which resulted in a temporary relocation of the overseers. An alternate location was made available within less than 24 business hours, despite pandemic staffing levels.

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 satisfactorily by the Treasury.

The EU review team had the opportunity to speak to Treasury staff as well as 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. They both provided a detailed presentation and replied to all subsequent questions raised by the team. The EU review team also received additional written information with sets forth the physical and technical security standards that applies to all sensitive compartmented information facilities. These standards facilitate the protection of sensitive compartmented information, including protection against compromise, emanations, inadvertent observation and overhearing, disclosure by unauthorised persons, forced entry, and the detection of surreptitious and covert entry.

Based on all this, the EU review team 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 US 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. 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 of 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. With the exception relating to an incident described below, all non-extracted data received prior to 30 November 2016 had already been deleted at the time of the review, in accordance with Article 6 (4) of the Agreement.

The incident was uncovered on 15 September 2020 and reported by the Treasury to the independent auditors contracted by the Designated Provider. The data was inadvertently saved during an auditor-witnessed copying of raw data during a storage migration. The auditors witnessed the deletion of the data on 22 September 2020 and verified that no backups exist. The Treasury explained that the out-of-scope data was not retained past the five-year period within the searchable database, and was deleted as scheduled from the searchable database on March 13, 2020. Per auditor requests, the U.S. Treasury Department added additional monitoring of the database containing the raw deliveries with daily notifications to the auditor.

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 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. The Treasury explained that no measures to identify unnecessary non-extracted data have changed since the 5th Joint Review. The Treasury stressed that it does not retain any non-extracted data past five years from the date received. It was also underlined that once a message type or geographic region is deleted from the Article 4 requests, all previous non-extracted data that had been received involving that message type or geographic region are permanently deleted during the course of a semi-annual deletion process.

Article 6 (2) requires that the Treasury should promptly delete any transmitted financial payment messaging data which were not requested. The Treasury confirmed that it was not aware of any such cases and stressed that there were strict oversight protocols in place that prevent the transmittal of payment messaging data without a request. Following an upgrade of the system on January 10, 2018 all non-extracted data older than five years to automatically deleted to ensure compliance with Article 6 (4). Independent program auditors monitor and confirm automatic process is conducted.

Article 6 (5) requires the Treasury to undertake an ongoing, 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. According to information received both orally and in writing from the Treasury, the TFTP system is since 10 January 2018 designed to automatically delete non-extracted data after five years. In addition, the Treasury assesses the data retention periods as part of the regular evaluation of the extracted data received described under 3.5 which includes investigators' interviews, reviews of counter-terrorism investigations, and an evaluation of current terrorist threats and activity. Based on its results, the Treasury is of the view that the current retention period is appropriate. The Joint Value Report adopted by the Commission on 27 November 2013 concluded that the reduction of the TFTP data retention period to less than five years

would result in a significant loss of insights into the funding and operations of terrorist groups.

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

The Treasury explained that, with regard to the disseminated information, it notifies law enforcement and partner agencies that receive leads derived from the TFTP information extracted from Provided 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, US 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 is 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. The Treasury explained that it is working to develop a functionality in its IT-system that will allow for the marking/unmarking of extracted data that has been viewed by an analyst for a short time, but not used (not generated a lead). The unmarked data would not be considered “extracted data” and, thus, would be automatically deleted after five years.

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) requires that the information extracted from Provided Data be deleted from the TFTP database, provided that the information is not being used for other specific investigations or prosecutions. In this context, the EU review team takes note of that Europol systematically, when disseminating leads encourages Member States to inform Europol and the Treasury of the follow up of cases regarding which it has received leads from the TFTP.

In the opinion of the EU review team, the issue of the retention of extracted data is exacerbated by the fact that the overwhelming majority of financial 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, but notes the anticipated IT-systems change that will minimise the "extracted data" to responsive records only.

The Treasury supplied 132 reports resulting from TFTP data to competent authorities of third countries during the review period. These reports generally summarise the results of an investigation of a subject and may contain multiple leads. Since the last joint review, all TFTP-derived information provided to third countries was provided pursuant to existing protocols on information sharing and based on prior consent between the United States and the relevant Member State. The Treasury underlined that it did not need to rely on a possible exception for the prevention of an immediate and serious threat to public security to share information without prior consent of the concerned Member States. The EU review team did not receive a list of the relevant third countries, but notes this is not required under the Agreement.

In light of the information provided by the Treasury, the EU review team is of the opinion that that retention and deletion of data pursuant to Article 6 is satisfactorily implemented. The EU review team welcomes the Treasury's work to develop functionalities to its IT system that would allow for the return of extracted data that is viewed by the Treasury analysts but not disseminated further in the context of a specific investigation to the database where it will be treated as non-extracted data and deleted after 5 years. However, the EU review team suggests that the Treasury establish written procedures for analysts' management of printed and electronic documents, and improve its mechanisms to review the necessity of retaining "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 (7)). When a case has been finally disposed of, this should lead to the deletion of extracted data relating to that case, unless there are other ongoing investigations based on the extracted data. The EU review team noted that the deletion of extracted data requires more extensive feedback from all counter-terrorism investigations on the use of TFTP- derived information.

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.

The EU review team suggests that the Treasury ensure that its website is subject to more regular updates, including of its section on questions and answers about the TFTP that includes value examples, to demonstrate that the programme remains valuable and relevant.

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 III 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[12] 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 EU review team 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.

The EU review team notes that the Privacy and Civil Liberties Oversight Board[13] ("PCLOB") is authorised to 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, and that the TFTP is subject to PCLOB's oversight authority. The PCLOB concluded in November 2020 an oversight review of the TFTP covering the period of January 2016 to November 2018. Following this review it issued a statement noting that its review indicates that TFTP is thoughtfully designed and not only provides significant value for counter-terrorism, but also appropriately protects individual privacy. In this context the PCLOB's staff provided four non-binding recommendations for Treasury's consideration: (1) provide consolidated, detailed written guidance to TFTP users; (2) provide additional guidance and training on identification and handling of US person information; (3) expand its internal privacy function and integrate privacy and civil liberties experts into the operation and oversight of TFTP; and (4) consider additional measures to promote compliance with privacy protections. The EU review team was informed that the Treasury is actively considering and addressing these recommendations as appropriate.

[12] The Article 29 Working Party ("Working Party on the Protection of Individuals with regard to the Processing of Personal data") was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR). The composition and purpose of the Working Party was set out in Article 29 of the Data Protection Directive (Directive 95/46/EC),

[13] https://www.pclob.gov/

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, including the absence of such data.

The Treasury has not received any Article 15 requests from a European NDPA wherein an individual sought to exercise the provisions described in Article 15 of the Agreement. As of December 31, 2021, the Treasury has received no requests pending pursuant to Articles 15 or 16 of the TFTP Agreement. In view of the absence of requests, it was not possible for the EU review team to assess the efficiency of the process for right of access set out in Article 15.

The Treasury explained to the review team the process and the technical aspects of preparing a thorough and correct response to a request. During the process , 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 EU review team encourages the Treasury to increase its efforts to raise awareness of the possibility to request access and 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 satisfactory.

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 EU and its Member States' law and under US law. During the review, only the US 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 US, so the possible options have not been asserted in practice.

Article 18 of 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 US 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 to seek administrative and judicial review of certain US Government agency 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 Judicial Redress Act of 2015[14], subject to designation by the US Attorney General,- extends to EU citizens certain core rights of judicial redress under Privacy Act of 1974.[15] EU citizens have legal standing before US Courts to file lawsuits in cases of refused access, rectification or unlawful disclosure of their personal data. This supplements 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 III), 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 US 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 US 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 EU Review team

[14] Public Law 114 - 126 - Judicial Redress Act of 2015
[15] Public law: 93-579 - Privacy Act of 1974

is overall 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 Treasury demonstrated that, in its annual evaluation of Article 4 Requests, it assesses the message types and geographic regions that are the most and least responsive to TFTP searches and takes the outcome of such an assessment into account in subsequent Article 4 requests, which results in updated requests that contribute to minimise the amount of data requested from the Designated Provider, in line with Article 4 (2). .The Joint Value Report in Annex IV provides for a list of concrete cases, in which TFTP data were used, and explains in the context of this review the added value of the TFTP.

The Commission services acknowledges the benefits of the close cooperation between the US 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 continue to remain independent from the verification role of Europol under Article 4 of the Agreement.

While the EU review team takes good note of the improvements in terms of efforts to minimise the amount of data requested from the Designated Provider and finds that the Article 4 Requests are narrowly tailored in accordance with the Agreement, it would welcome more updated explanations on the value of keeping the selected message types when sending new Article 4 Requests.

The EU review team further suggests that the Treasury improve its mechanisms to review the necessity of retaining "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 (7)). This could include documentation setting out the processes and controls in place to evaluate the value of extracted data. In this context, it is important that Member States increase their efforts 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, unless thare are other investigations based on the extracted data. Particular attention should be provided to extracted data that is viewed by the Treasury analysts, but not disseminated further in the context of a specific investigation.

As already stated in the last review, Member States' regular feedback to Europol, for onward sharing with the Treasury as appropriate, on the added value of the TFTP leads received from the Treasury could further improve the quality and the quantity of information exchanged under Articles 9 and 10. In addition, Europol is encouraged 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 services invite the Treasury and Europol to consider ways to facilitate the processing of leads, in compatibility with the security arrangements of the TFTP.

The Commission services note that the procedures to process requests from persons whether their data protection rights have been respected in compliance with procedure set out in the Agreement appear to function efficiently. However, the Commission services suggest that the Treasury ensure that such verifications 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. The Commission services underline the importance of that the Privacy Officer of the U.S. Treasury Department, charged with the implementation of Articles 15 and 16 of the Agreement, continue its efforts to make right of access and redress more available to persons and consider how procedures can tested in the absence of specific requests

A regular review of the Agreement is essential to ensure its proper implementation, to build up a relationship of trust between the contracting parties and to provide reassurances to interested stakeholders on the usefulness of the TFTP instrument. It was agreed to carry out the next joint review according to Article 13 of the Agreement in the beginning of 2024.

Annex I – Composition of the review teams

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

- Mr. Laurent Muschel, Director Internal, Security, Directorate-General Migration and Home Affairs, European Commission, Head of the EU Article 13 review team
- Mr. Bertil Vaghammar Policy Officer, Counter Terrorism, Directorate-General Migration and Home Affairs, European Commission
- Ms. Ines Walburg, Head of a division, 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 **United States team** were:

- Ms. Lisa Palluconi, Associate Director, Office of Foreign Assets Control, U.S. Department of the Treasury (Head of U.S. delegation)
- Mr. Brandon Lee, Senior Sanctions Policy Advisor, Office of Foreign Assets Control U.S. Department of the Treasury
- Ms. Anu Madan, Sanctions Investigator, Office of Foreign Assets Control, U.S. Department of the Treasury
- Mr. John Snodgrass, Attorney-Advisor, Office of the General Counsel, U.S. Department of the Treasury
- Ms. Lauren Bernick, Principal Deputy Chief, , Office of Civil Liberties, Privacy , and Transparency, Office of the Director of National Intelligence
- Mr. Dylan Cors, International Director, National Security Division, U.S. Department of Justice
- Mr. Ken Harris, Senior Counsel for European Union and Multilateral Criminal Matters, U.S. Department of Justice

Annex II – Europol statistical information

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

Period	December 2018 – November 2021				
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[16]	Verification	Number of pages
Dec-18	04/12/2018	157		05/12/2018	178
Jan-19	09/01/2019	154		10/01/2019	174
Feb-19	07/02/2019	156		08/02/2019	177
Mar-19	13/03/2019	142		14/03/2019	163
Apr-19	09/04/2019	144		11/04/2019	165
May-19	07/05/2019	145		08/05/2019	164
Jun-19	12/06/2019	146		13/06/2019	166
Jul-19	09/07/2019	149		11/07/2019	180
Aug-19	07/08/2019	123		09/09/2019	144
Sep-19	10/09/2019	126		11/09/2019	147
Oct-19	08/10/2019	128		09/10/2019	151
Nov-19	05/11/2019	128		06/11/2019	152
Dec-19	04/12/2019	129		05/12/2019	153
Jan-20	08/01/2020	125		09/01/2020	148
Feb-20	05/02/2020	123		06/02/2020	151
Mar-20	03/03/2020	122		04/03/2020	148
Apr-20	n/a[17][18]	-	-	-	-
May-20	n/a	-	-	-	-
Jun-20	29/06/2020	125		01/07/2020	151
Jul-20	n/a	-	-	-	-
Aug-20	05/08/2020	125		06/08/2020	153
Sep-20	14/09/2020	128	-	15/09/2020	156
Oct-20	06/10/2020	121	-	07/10/2020	151
Nov-20	09/11/2020	121	-	10/11/2020	152
Dec-20	08/12/2020	123	-	09/12/2020	160
Jan-21	19/01/2021	126	-	20/01/2021	161
Feb-21	10/02/2021	129	-	11/02/2021	165

16 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.

17 No Article 4 production order (Request) was sent during the U.S. Treasury Department's "mandatory telework policy" period during the covid-19 pandemic (Treasury employees were required to work remotely.

18 A slight deviation in protocol for the delivery and review of Article 4 Requests for the periods of April and May 2020 was memorialized in an April 27, 2020 memorandum to Europol, in consultation with the European Commission and the Designated Provider.

Mar-21	03/03/2021	134	-	04/03/2021	171
Apr-21	07/04/2021	135	-	08/04/2021	173
May-21	05/05/2021	136	-	06/05/2021	175
Jun-21	08/06/2021	145	-	09/06/2021	184
Jul-21	07/07/2021	146	-	08/07/2021	184
Aug-21	03/08/2021	145	-	04/08/2021	183
Sep-21	08/09/2021	146	-	09/09/2021	184
Oct-21	06/10/2021	147	-	07/10/2021	185
Nov-21	09/11/2021	148	-	10/11/2021	186
		136 Average (rounded)			155 Average (rounded)

B. Summary of monthly figures (as per 1 December 2018)

2018

Month	01 2018	02 2018	03 2018	04 2018	05 2018	06 2018	07 2018	08 2018	09 2018	10 2018	11 2018	12 2018
Article 4												1
Article 9[19]												0
Article 10[20]												23

2019

Month	01 2019	02 2019	03 2019	04 2019	05 2019	06 2019	07 2019	08 2019	09 2019	10 2019	11 2019	12 2019
Article 4	1	1	1	1	1	1	1	1	1	1	1	1
Article 9	4	1	8	3	4	0	1	1	14	3	5	4
Article 10	10	14	14	12	19	33	17	9	23	20	23	11

2020

Month	01 2020	02 2020	03 2020	04 2020	05 2020	06 2020	07 2020	08 2020	09 2020	10 2020	11 2020	12 2020
Article 4	1	1	1	0	0	1	0	1	1	1	1	1
Article 9	4	1	1	0	0	0	0	3	0	0	1	1
Article 10	14	19	16	26	15	25	6	13	8	9	15	11

2021

Month	01 2021	02 2021	03 2021	04 2021	05 2021	06 2021	07 2021	08 2021	09 2021	10 2021	11 2021	12 2021
Article 4	1	1	1	1	1	1	1	1	1	1	1	
Article 9	0	0	0	0	0	0	0	0	0	5	2	
Article 10	3	8	13	9	11	5	8	9	6	15	16	

19 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).

20 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

12/2018 – 11/2021 (review period)	Sum
Article 4	33
Article 9	66
Article 10	508

Article 10 requests				
Requester	2018 (12/18)	2019	2020	2021(11/21)
EU Member States	19	178	166	93
Europol	4	27	11	10
Eurojust	0	0	0	0
Total	23	205	177	103

D. Summary of intelligence leads (overall, as per 30 November 2021)

Article 9: Information spontaneously provided by the US	
Instances	**Leads**
238	21 403
Article 10: Requests for searches	
Requests	**Leads**
1297	132 220
Article 10 Requests – Referrals by US DoT[10]	
44	

E. Use of TFTP in relation to the phenomenon of foreign fighters (overall, as per 30 November 2021)

Article 9: Requests for searches	
Requests	**Leads**
146	21 615
Article 10: Requests for searches	
Requests	**Leads**
479	52 663

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

EU questionnaire for the Sixth joint review of the EU-US TFTP agreement (January 2022)

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 covered the period from 1 January 2016 to 30 November 2018. The sixth review will cover the period from 1 December 2018 to 30 November 2021.

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 sixth 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 three previous 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 total number of financial payment messages received from the Designated Provider has been slightly higher over the course of the 36-month period between December 1, 2018 and November 30, 2021 ("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 29 807 searches of data provided by the Designated Provider, for an average of 828 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, most 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-party countries has increased during the review period. Please see the responses to Questions 4, 5, 10, and 11 below. The U.S. 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 530 TFTP-derived reports consisting of 10884 leads pursuant to Article 9, and an additional 47 845 leads pursuant to Article 10, to competent authorities of EU Member States and Europol. A TFTP "lead" refers to the summary of a particular financial transaction identified in response to a TFTP search that is relevant to a counter-terrorism investigation. A single TFTP report may contain multiple TFTP leads. For example, one Article 9 spontaneous report provided to Europol during the review period contained 507 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 a situation, 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 came from the TFTP. Since the Agreement entered into force in August 2010, the U.S. Government has continued to use reports as the vehicle for the spontaneous provision of information to the competent authorities of EU Member States and Europol pursuant to Article 9. Article 9 reports provided to Europol are explicitly identified as containing TFTP-derived information.

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

   U.S. investigators supplied 132 reports, including Article 10 and Article 9 reports, resulting from 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.

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

   Article 7(d) authorizes the sharing of certain information involving EU persons *"subject to the prior consent of competent authorities of the concerned Member State or pursuant to existing protocols on such information sharing between the U.S. Treasury Department and that Member State."* Since the last joint review, all TFTP-derived information provided to third countries was provided pursuant to existing protocols on information sharing between the United States and the relevant Member State.

   In the event information could not be shared pursuant to existing protocols, the U.S. Treasury Department would not disseminate the information without prior consent of the concerned Member States except where the sharing of the data was essential for the prevention of an immediate and serious threat to public security. Because the U.S. 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, the Fourth Review in March 2016, and the Fifth Joint Review in January 2019.

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. *(attached as Annex IV)*

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 U.S. 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 U.S. 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 U.S. 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, 66 reports consisting of 10 884 TFTP leads were provided to EU Member States and Europol as the spontaneous provision of information pursuant to Article 9.

The U.S. Treasury Department has received positive feedback from Europol and certain EU Member States about the value of the U.S. Treasury Department's provision of TFTP-derived information and its significant impact on European counter-terrorism investigations. However, it is uncommon for EU Member States or Europol to provide the U.S. Treasury Department with analytic "follow-on information" in response to the provision of information pursuant to Articles 9 and 10. The U.S. Treasury Department appreciates Europol's ongoing efforts to encourage EU Member States to provide feedback, where possible, to the U.S. 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 feedback to the US Treasury Department on that information coming from EU-MS or Agencies?**

The U.S. Treasury Department received 508 requests from EU Member States and Europol pursuant to Article 10 during the review period and responded to all 464 requests that had an overseer-approved nexus to terrorism. 44 Article 10 requests required additional information to substantiate a nexus to terrorism, which were not able to be processed by the U.S. Treasury Department during the period of review. All Article 10 requests are reviewed by both the data provider overseer and the EU overseer prior to performing searches to maintain compliance with the Agreement. TFTP searches resulted in the transmission of leads to the EU in response to 262 of the 464 requests.

There were 47 845 leads contained in the 262 Article 10 responses provided to EU Member States and Europol during the review period. Throughout the period of review, Europol provided the U.S. Treasury Department with EU Member States' feedback regarding TFTP information that provided significant leads to European CT investigations via 15 Article 10 responses.

12. **How has the COVID-19 pandemic effected the safeguards, controls and reciprocity provisions set out in the Agreement? Please describe how the pandemic effected the number of financial payment messages accessed and the number of occasions on which leads have been shared with Member States, third countries, Europol and Eurojust.**

The COVID-19 pandemic did not materially affect the safeguards, controls, or reciprocity provisions set out in the Agreement. The U.S. Treasury Department worked in tandem with Europol to develop a schedule for information sharing that is safe and cohesive for both parties. Overseer, auditor, and security oversight were not affected except in terms of adjusting staffing levels. Live and retroactive review of system access and searches conducted on system were available and functioning during the period of review. Liaison meetings with Europol were reduced to weekly meetings due to reduced staffing levels. During the U.S. Treasury Department's "mandatory telework policy" period (in which Treasury employees were required to work remotely, from March 2020 to May 2020), the U.S. Treasury Department responded to 48 Article 10 requests with a total of 3 572 leads. This included two priority and one urgent Article 10 requests. The number of searches on the system were reduced during the mandatory telework period in 2020 by a reduction of 54% from 2019 and 33% from 2021. This reduction in searches is also attributed to some residual impact resulting from reduced staffing due to the U.S. Treasury Department's "maximum telework policy" (in which Treasury employees are strongly encouraged to telework to the maximum possible extent, from June 2020 to present), which remained in effect throughout the remainder of the review period.

III. Implementation and effectiveness of the Agreement

13. **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. Treasury Department has not collected financial payment messages from the Designated Provider in the EU, except as authorized by the TFTP Agreement. Moreover, during that time, the U.S. Treasury Department has not served any subpoenas on the Designated Provider in the EU or in the United States requesting the production of data stored in the EU, except as authorized by Article 4 of the TFTP Agreement. The U.S. 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.

14. **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. Please see the response to Question 15 regarding a slight deviation in protocol for the delivery and review of Article 4 Requests for the periods of April and May 2020.

15. **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 U.S. Treasury Department submitted its Article 4 Requests on a monthly basis, with the exception of a slight deviation in the first months of the global COVID-19 pandemic, when the U.S. Treasury Department was subject to mandatory telework. The protocol for the delivery of the Article 4 Requests for the periods of April 2020 and May 2020 was memorialized in an April 27, 2020 memorandum to Europol, in consultation with the European Commission and the Designated Provider, which Europol confirmed on April 30, 2020 and further modified on June 4, 2020. There have been no such deviations in the reporting during the review period.

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 U.S. 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 — to provide additional information relating to the provisions of Article 4 regarding the necessity of the data and terrorism-related threats and vulnerabilities.

16. **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 U.S. 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 susceptible to relevant terrorist activity. In tandem with this regular review, the U.S. 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 U.S. Treasury Department completed two annual evaluations. The U.S. Treasury Department submitted the 2018 annual evaluation on March 6, 2020, and the joint 2019-2020 evaluation on May 4, 2021. These 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 U.S. Treasury Department made certain streamlining adjustments that resulted in a more tailored Request containing the most recent and relevant data. During the 2019-2020 evaluation, the U.S. Treasury Department recommended adding three jurisdictions to the Requests to counter the threat posed by Racially or Ethnically Motivated and Violent Extremists (REMVE) and removing three jurisdictions from the Requests that were of less value than others for purposes of prevention, investigation, detection, or prosecution of terrorism or its financing. OFAC also recommended

removing two Message Types that provided leads of only limited utility. Only 17% of all Message Types are extracted for use in TFTP. In addition, the U.S. Treasury Department has continued to streamline the Article 4 to include the most relevant information and most recent supporting evidence. The U.S. Treasury Department will be conducting its annual evaluation covering January 2021–December 2021 during the first half of 2022. This annual evaluation will assess the impact of the removal of the three jurisdictions and whether circumstances justify their inclusion in the future.

The U.S. 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 analysis.

17. **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 U.S. Treasury Department Request and supplemental documents. Please see the response to Question 15 regarding a slight deviation in protocol for the delivery and review of Article 4 Requests for the periods of April and May 2020.

18. **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 U.S. 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 U.S. Treasury Department with respect to Requests submitted pursuant to Article 4(1), apart from a 30 April 2020 request from Europol for an assessment of any additional terrorism threats from the so-called Islamic State due to the COVID-19 pandemic. The U.S. Treasury confirmed that the scope of the provided Article 4 Request appropriately accounted for such threats.

During the summer of 2011, the U.S. Treasury Department and Europol agreed that Europol would notify the U.S. 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 U.S. 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 U.S. Treasury Department has carefully considered these suggestions and has generally adopted them.

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

The U.S. Treasury Department assesses that the Agreement is important and effective in supporting European and global counter-terrorism efforts, particularly in light of the heightened terrorist threat to Europe.

The U.S. 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.

20. **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? Has the oversight mechanism resulted in any recommendations?**

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 Department of the Treasury's 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, although due to system improvements OIG is no longer required to oversee the deletion of data.

Similarly, in addition to the OIG, the U.S. Treasury Department's Office for Privacy, Transparency, and Records provides verifications regarding the Treasury Department's implementation of the TFTP Agreement. The Office of the 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 21, 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 U.S. Treasury Department's counter-terrorism functions, which can include the TFTP, and U.S. Treasury Department officials periodically brief the Committees on these issues.

Finally, the Privacy and Civil Liberties Oversight Board ("PCLOB") is an independent agency within the Executive Branch of the U.S. Government. PCLOB 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 counter-terrorism program, TFTP is subject to PCLOB's oversight authority. How PCLOB independently elects to exercise its oversight authorities with respect to TFTP is, of course, up to PCLOB. In November 2020, PCLOB concluded an oversight review of the TFTP covering the period of January 2016 to November 2018. PCLOB requested and reviewed certain documentation and conducted briefings with U.S. Treasury Department officials. PCLOB's Chairman issued a statement noting that "[t]he Board's review indicates that TFTP is thoughtfully designed, provides significant value for counter-terrorism, and appropriately protects individual privacy." PCLOB provided four

recommendations for Treasury's consideration. The recommendations were: (1) provide consolidated, detailed written guidance to TFTP users; (2) provide additional guidance and training on identification and handling of U.S. person information; (3) expand its internal privacy function and integrate privacy and civil liberties experts into the operation and oversight of TFTP; and (4) consider additional measures to promote compliance with privacy protections. The U.S. Treasury Department is actively considering and addressing these recommendations as appropriate.

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

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

The U.S. 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 (when the U.S. Treasury Department receives inquiries related to TFTP) and Office of Foreign Assets Control ("OFAC"), the Privacy Officer has 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 U.S. Treasury Department's website at www.treasury.gov/tftp. To avoid potential conflicts, the Privacy Officer is not involved in the daily functioning of the TFTP or review of every search done on the system, to avoid a potential conflict of interest.

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 perfected 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,[21] along with the Inspector General of the Treasury Department, have oversight with respect to the program.

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

Treasury has not identified any new issues during the reporting period. Prior to the 2019 Joint Review, U.S. 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 a 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 necessary to ensure the identity of requesters and reduce the risk of unauthorized disclosures of personal data.

During the review period, the U.S. Treasury Department has not received any Article 15 or Article 16 requests under the agreement.

23. **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 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 multi-layered set of systems and controls previously reviewed remains in place to ensure that provided data is processed exclusively for the prevention, investigation, detection, or prosecution of terrorism or its financing, and that all searches of provided data is 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:

[21] The Treasury Department's Office of the 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: reviewing the Request to the Designated Provider and associated supplemental documents provided to Europol to ensure they meet the standards of Article 4; responding to questions regarding the legal sufficiency of a search justification and its associated query to ensure that they satisfy the standards of Article 5; providing legal guidance regarding the retention and deletion requirements of Article 6, including the necessity-based review; and reviewing dissemination requests to ensure they comply with the standards of Article 7.

- All analysts who have access to the TFTP system are extensively trained and re-trained regularly to ensure the fulfilment of all requirements for searches, including that a pre-existing nexus to terrorism or its financing is documented for every search; if an analyst even attempted a search that did not satisfy the requirements, the U.S. 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 TFTP;

- 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; for example, 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.

  We note that, during the current review period, the overseers' workspace experienced flooding, which resulted in the temporary relocation of the overseers. Access to oversight was promptly made available even given the challenges of needing to quickly procure a secure location for the overseers and navigating the U.S. Treasury Department's COVID-19 protocols, which limited in-person office work. The U.S. Treasury Department made an alternate location available within less than 24 business hours, despite pandemic staffing levels.

24. **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 23, above, prevent any type of data mining or profiling because they require individualized searches, based on a pre-existing nexus to terrorism or its financing. No additional measures have been put into place since the 5th Joint Review.

25. **Have any measures been put in place to implement the provisions of Article 5(4) on data security and integrity or have any measures been changed since the last Joint Review? If so, what changes have occurred? In particular, can you confirm: that the provided data is held in a secure physical environment, stored separately from other data and that there are no interconnections with any other database?**

Multiple physical and technical security layers exist to ensure data security and integrity. The data is 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 is 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.

26. **Have there been any cases of incidents that could affect the security and integrity of TFTP data? If so, have any technical and organisational measures put in place to address such security incidents, including notification?**

No instances have been detected. TFTP data is held in a secure physical environment, stored separately from other data on a standalone system with no interconnections with any other database and protected by high-level systems and physical intrusion security controls. As such, TFTP data was not impacted by reported cyber-related attacks on U.S. government departments and agencies that occurred during the review period.

27. **Have the measures put in place to implement the provisions of Article 5(4) been subject to oversight defined in Article 12 (1) of the Agreement?**

Yes. The Designated Provider has three full time staff, who are independent contractors and monitor all access. The Designated Provider has one full time and three part time overseers who provide oversight of duties mentioned in 12(1). The EU has an overseer who fulfils the functions of Article 12(1) who has been provisioned access.

28. **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 U.S. 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 responses to Question 23, above, and Question 38, below.

29. **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 23, above.

30. **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 U.S. Treasury Department is not aware of any cases in which such data have been extracted.

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

No measures to identify unnecessary non-extracted data have changed since the 5th Joint Review. The U.S. Treasury Department does not retain any non-extracted data past five years from the date received.

Additionally, the U. S. Treasury Department is in the developmental stage of creating a mechanism for analysts to further narrow the scope of the data extracted from search results. This system enhancement is expected to reduce the amount of data retained.

32. **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, the U.S. Treasury Department is not aware of any cases in which financial payment messaging data was transmitted which was not requested. There are strict oversight protocols in place that prevent the transmittal of payment messaging data without a request. Additionally, the system was upgraded on January 10, 2018 to automatically delete non-extracted data older than five years. Independent program auditors monitor and confirm automatic process is conducted.

33. **Have all non-extracted data received prior to 30 November 2016 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 September 15, 2020, the U.S. Department of the Treasury alerted the Designated Provider's contract auditors that data was inadvertently retained in the April 23, 2015 delivery. The data contained raw unprocessed Designated Provider data, covering messages from the period March 3, 2015 through April 8, 2015, which was

older than five years at the time identified. The data was inadvertently saved during an auditor-witnessed copying of raw data during a storage migration. The auditors witnessed the deletion of the data on 22 September 2020 and verified that no backups exist. The out-of-scope data was not retained past the five-year period within the searchable database and was deleted as scheduled from the searchable database on March 13, 2020. Per auditor requests, the U.S. Treasury Department added additional monitoring of the database containing the raw deliveries with daily notifications to the auditor. Other than this incident, all non-extracted data received prior to November 30, 2016 was deleted in accordance with Article 6(4) of the Agreement.

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

The U.S. 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 16, 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 appropriate to ongoing counter-terrorism efforts. Based on past annual evaluations completed since the Agreement entered into force, as well as the ongoing assessments, the U.S. 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.

35. **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 33, above, and 36, below.

36. **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?**

The TFTP system is designed to automatically delete non-extracted data after five years. This process is conducted in a way that ensures the system remains fully operational and all safeguards remain in place. This system upgrade was completed and implemented on January 10, 2018. Independent program auditors monitor and confirm automatic process is conducted.

All non-extracted data received prior to November 30, 2016 has been deleted. See Question 33 for additional information on process improvements to ensure old data is removed if or when such data is transitioned between storage areas.

37. **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? Have there been any cases of onward transfer of information involving citizens or residents of EU Member States?**

No changes have occurred since the last Joint Review. Onward transfer of information occurred during the period of review, some of which involved citizens or residents of

EU Member States. Any onward transfers of information involving citizens or residents of EU Member States would be protected by the information sharing agreements between the US and the receiving country. The onward transferred information can only be used for counter-terrorism lead purposes and is marked with appropriate caveats and handling instructions, as with all TFTP information.

38. **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 U.S. Treasury Department.

In cases in which the U.S. 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 U.S. Treasury Department abides by the existing protocols on information sharing with that Member State. In cases where existing protocols do not exist, the U.S. Treasury Department will not disseminate the information without prior consent of the Member State except where the sharing of data is essential for the prevention of an immediate and serious threat to public security.

39. **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. During the first quarter of 2020, overseers' schedules were alternated to ensure oversight activities were not affected by COVID-19 restrictions. See Question 23 for additional information regarding the temporary relocation of the overseers due to workspace flooding.

40. **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 counter-terrorism purpose limitation and other safeguards described in Articles 5 and 6 of the Agreement. The overseers may request additional justification or clarification of the counter-terrorism nexus as well as documentation to ensure that the search is as narrowly tailored as possible. In the overwhelming majority of cases, the overseers request additional information simply for routine auditing purposes and not out of any concern with the search itself.

During the review period, the overseers queried 697 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 97.66%), the overseers were fully satisfied with the search as formulated. The overseers stopped 22 searches at the time of the search and, of all searches queried, blocked 92 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 (22 total searches during the 36 months of the review period or 0.07% 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 697 searches queried, the U.S. 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 having been queried by the overseers generally.

41. **In how many cases have the overseers queried or stopped searches on the grounds that they appear to be in breach of Article 5 of the Agreement? How many searches were finally identified, possibly on the basis of additional information, as not being in line with the Agreement? What are the typical reasons for intervention by the overseers and what measures are taken to ensure compliance with the Agreement?**

As noted in response to Question 40, above, in a small number of cases the overseers either stopped or blocked the searches (114 total searches during the review period or 0.38%). Fifty-one percent of the stopped or blocked searches were due to overbroad search terms, a typographical error in the spelling of a terrorism suspect's name, or the inadvertent transposition of two digits in a bank account number. Forty-nine percent of stopped or blocked searches were determined to have an insufficient nexus to terrorism, meaning the subject was too far removed from the nexus to terrorism and the search was therefore deemed overly broad.

As noted in response to Question 23, above, all analysts who have access to the TFTP are extensively trained and re-trained regularly to ensure the fulfilment of all requirements for searches. When an analyst attempts a search that does not satisfy the requirements, the U.S. 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 U.S. Treasury Department may also permanently revoke an analyst's access rights to the TFTP or institute disciplinary proceedings, although the U.S. Treasury Department has not needed to exercise these options to date.

42. **Have any measures been 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 U.S. Treasury Department. The U.S. 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.

43. **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 U.S. Treasury Department has not received any Article 15 requests from European NDPAs during the current review period.

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 U.S. 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. The DASPTR also advised the requester of that they may seek judicial review of the decision by filing suit in the United States District Court for the District of Columbia and explained in further detail why additional information beyond a statement that the requester's rights had been respected under the agreement could not be provided.

Judicial redress under U.S. law would consist of seeking redress in federal court from an adverse administrative action and the United States has defences to such a suit. 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. As of December 31, 2021, the U.S. Treasury Department has received no requests pending pursuant to Articles 15 or 16 of the TFTP Agreement.

44. **Have those access requests been answered positively, including the disclosure of personal data processed under the Agreement? 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 2019 Joint Review, Treasury received no requests pursuant to Article 15 or Article 16 of the TFTP Agreement.

45. **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 U.S. Treasury Department is not aware of any instance in which inaccurate data was received or transmitted pursuant to the Agreement.

46. **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.

47. **Were any notifications and consultations regarding cases of personal data processed in breach of the Agreement made by either of the Parties as set out in Article 18(1) of the Agreement? If so, please elaborate.**

    No.

48. **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?**

    No.

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 IV – Examples of cases in which TFTP has been used for the prevention, investigation, detection, or prosecution of terrorism or its financing

EU Value Examples: 2019-2021

The Terrorist Finance Tracking Program (TFTP) is a vital counter-terrorism tool that provides valuable lead information that helps discover planned terrorist attacks and has been used in the investigation of numerous actual and attempted terrorist attacks. 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. TFTP provided key leads, as well as the various methods in which TFTP-derived data helped identify the financial support networks behind terrorist organisations currently under investigation by U.S. and European authorities. The examples below highlight cases in which the U.S. Treasury Department provides spontaneous counter-terrorism information to Europol (Article 9) and when Europol request the U.S. Treasury Department for certain counter-terrorism information (Article 10).

2019

- TFTP data was used to develop leads in Operation Ring, a Spanish investigation of a network moving money, via money service business (MSB) remittances and traditional banking channels, from Spain and other EU Member States to support Islamic State of Iraq and the Syria (ISIS) activities in Syria. TFTP-derived data assisted with the identification of terrorist financers and supporters within the principal suspect's network, as well as helped develop new lines of investigation. Spanish investigators issued European Arrest Warrants and Letters of Request relating to other possible terrorist financiers linked to the network. Additionally, Analysis Project-TFTP (AP-TFTP)[22] assisted in intelligence collection efforts. This operation is ongoing with Spanish judicial authorities. (Article 9, Belgium, Italy, Spain, and Europol)

- TFTP data assisted in Operation Poppins, an ongoing Spanish law enforcement investigation into a network of individuals in Ceuta, Spain and Belgium suspected of terrorist financing. The investigation uncovered a network in which funds were transferred, via MSB remittances, between certain EU Member States and Turkey to fund ISIS activities. TFTP data assisted in uncovering the transactional flow of funds and the suspects involved. (Article 10, Spain)

- TFTP data was used in Operation Picnic, an Irish investigation of a network of suspects in Ireland, Turkey, Pakistan, Lebanon, and Uzbekistan, who financed and supported Al-Qaeda activities via money transfers through traditional banking channels using the accounts of relatives. This investigation remains ongoing, however 11 individuals have been detained and/or arrested. (Article 10, Ireland)

[22] AP-TFTP is a project to help detect the financing of terrorism. Analysis Projects (APs) are analytical projects within the Europol Analysis System – an information processing system-and focus on certain crime areas from commodity-based, thematic, or regional angles (e.g., drug trafficking, Islamist terrorism, Italian organized crime).

- TFTP data was used by Hungary's counter-terrorism unit in the investigation of the financing of terrorism activities, through privately owned business. This investigation led to the conviction and imprisonment of two Kurdish nationals who were members of the outlawed Kurdistan Workers Party in northern Iraq, an identified terrorist organization. The convicted individuals were expelled from Hungary for eight years. (Article 10, Hungary)

2020

- TFTP leads assisted with Operation Sirte, a Spanish-based investigation into the smuggling of oil to finance terrorism-related activities for local militias in Libya. These local militias control certain areas in which the petroleum is mined and smuggled. Additionally, Operation Sirte provided leads, some of which were TFTP derived, that assisted with Operation Dirty Oil, a transnational investigation led by Guardia di Finanza, an Italian law enforcement agency. This investigation resulted in more than ten arrest. (Article 10, Spain and Italy)

- TFTP data assisted the Syrian Wallet Operation, an ongoing EU-US project that investigates suspects of financing terrorist operations within EU Member States and providing financial assistance , via MSB remittances, to terrorist activities in Syria. AP-TFTP received to the Western Balkan financiers of terrorism. Several Member States initiated independent investigations based upon this operation, which assisted in arrest of some terrorist suspects. (Article 9, Belgium, Italy, Spain, and Europol)

- TFTP information was provided in developing the framework for Operation Bleating, an investigation internationally coordinated by Europol. Operation Bleating investigated suspects of providing financial support, via MSB remittances, to terrorist groups linked to ISIS in African countries. Some of the individuals identified through the TFTP data are known conduits for ISIS operations in Europe, Africa, and the Middle East and belong to the Rawi Network. Additionally, these individuals linked to the Rawi Network are designated pursuant the U.S. Treasury Department's terrorism authorities. (Article 10, Europol)

- TFTP information was used in Operation Soldi, which is a transnational investigation conduct in Switzerland and internationally coordinated by Europol with other EU Member States. Operation Soldi resulted in judicial proceedings against some Swiss citizens who were accused of having transferred large sums of money into Syria to fund ISIS financiers of terrorism. The money was moved via banking transmissions and remittances via MSBs. The TFTP data provided generated new leads for Operation Soldi. Additional information sharing with other parties, uncovered a wider network of MSBs in Germany, Spain, and France. (Article 10, Europol, Germany, Spain, and France)

2021

- Throughout much of 2021, Austrian law enforcement officials conducted an investigation to identify potential leads connected to Kujtim Fejzulai, who on February 11, 2020 killed five (including himself) and injured 15 individuals during a terrorist attack in Vienna. In support of this investigation, the U.S. Treasury Department provided 237 TFTP leads containing valuable financial intelligence to

Europol and Austrian law enforcement. (Article 10, Austria)

Since July 2021, certain EU Member States have conducted an investigation into ten non-profit organizations based the Benelux Union that were suspected of providing financial support to terrorist organizations such as Hamas. The U.S. Treasury Department provided 502 TFTP leads that linked purportedly "humanitarian-related" transactions that in fact funded terrorist-related activities to entities certain jurisdictions, including the UK, Turkey, and Lebanon. This investigation is ongoing. (Article 10, Netherlands)

- TFTP data was used in Operation Combating the Financing of Terrorism (CFT), which revealed a terrorist network operating within certain EU Member States, Syria, and Iraq. Operation CFT uncovered a network of individuals purchasing anonymized prepaid coupons at licensed tobacco shops, known as Tabacs, in France and outside the EU to finance terrorist activities. The anonymized prepaid coupons were then converted into cryptocurrencies (via digital asset service providers) to finance Al-Qaeda related activities. This operation resulted in 29 arrest. (Article 10, France)

- The European Counter Terrorism Centre developed Terrorist Identification Task Forces (TITF), which collects information used to target terrorism suspects within EU Member States. The second phase of TITF investigated suspects with ties to Hizballah. The U.S. Treasury Department provided 681 TFTP leads that assisted in the investigation of a Europe-based Lebanese Hizballah fundraising network. The network involved wealthy suspects with ties to Iran, who provided financial support to the Lebanese Hizballah fundraising network through seven Islamic charities based throughout Europe. This investigation is ongoing. (Article 10, Europol)

- Since January 20201, an EU Member States' Counter-Financing of Terrorism Unit investigated several suspects of providing financial support to ISIS. TFTP data was used to identify one of the suspects located in Turkey (having a Canadian passport), who raised money for the terrorist organization. The financial transactions were listed as donations for certain companies or donations for "educational purposes" to entities linked with Islamic education, allegedly involved in financing terrorist activities. This investigation is ongoing. (Article 10, Belgium, Netherlands)

US Value Statement Summary, TFTP 6th Joint Review

The Terrorist Finance Tracking Program's (TFTP) 6th Joint Review was held at the U.S. Department of the Treasury March 29 - 30, 2022. The Joint Review consisted of delegations from the U.S. Department of the Treasury and the European Union. During the review, ten TFTP-derived value examples were shared in order to illustrate the usage and utility of the data. The value examples highlighted the importance of TFTP data in terrorism investigations. The examples ranged from complicated cross-border terrorism financing schemes to querying TFTP data to identify subjects' involvement in transactions and/or activities regarding terrorism. In all examples, TFTP analysts used TFTP data to build networks and inform investigations. Additionally, during the period of review, TFTP data

directly informed six U.S. Department of Treasury Specially Designated Global Terrorist designations.

TFTP data has been used to support U.S. law enforcement and sanctions-related investigations involving terrorism and terrorist financing. For example, the U.S. Department of the Treasury used TFTP information in several counter-terrorism sanctions investigations, including those resulting in: the September 2018 designation of a Kenya-based facilitator for the Islamic State of Iraq and Syria; the July 2019 designation of a Jama'at Nusrat al-lslam wal-Muslimin leader who was involved in the March 2019 attack on Mali Armed Forces; the December 2019 designation of a network of prominent Lebanon and the Democratic Republic of Congo (DRC)-based Hizballah money launderers; the September 2021 designation of a network of Hizballah financiers, financial facilitators, and senior officials in Qatar, Kuwait, and Lebanon; and the January 2022 designation of Zambia-based companies leveraged by two Lebanon-based Hizballah financiers.