



The United States Department *of the* Treasury

TERRORIST FINANCE TRACKING PROGRAM

Questions and Answers

After the terrorist attacks on September 11, 2001, the United States Department of the Treasury initiated the Terrorist Finance Tracking Program (TFTP) to identify, track, and pursue terrorists – such as Al-Qaida – and their networks. An agreement between the European Union (EU) and the United States (US) on the transfer and processing of data for purposes of the TFTP entered into force on August 1, 2010. This document is intended to answer many of the most common questions about the TFTP and the Agreement.

Q.1: What is the value of the TFTP?

A.1: Since its inception in 2001, the TFTP has provided valuable lead information that has aided in the prevention of many terrorist attacks and in the investigation of many of the most visible and violent terrorist attacks and attempted attacks, including, for example:

- the November 2015 attacks in Paris and raid in Saint-Denis;
- the January 2015 attack in Paris and anti-terrorism raid in Verviers;
- the 2013 Boston Marathon bombings;
- threats to the 2012 London Summer Olympic games;
- the 2011 plot to assassinate the Saudi Arabian Ambassador to the US;
- the 2011 attacks in Norway conducted by Anders Breivik;
- the Nigerian Independence Day car bombings in Abuja, Nigeria in 2010;
- the Jakarta hotel attacks in 2009;
- hijacking and hostage operations by Al Shabaab, including the hijacking of the Belgian vessel MV Pompei in 2009;
- the attacks in Mumbai in 2008;
- the Islamic Jihad Union plot to attack sites in Germany in 2007;
- the plan to attack New York's John F. Kennedy airport in 2007;
- the liquid bomb plot against transatlantic aircraft in 2006;
- the bombings in London in 2005;
- the Van Gogh terrorist-related murder in the Netherlands in 2004;
- the Madrid train bombings in 2004; and
- the Bali bombings in 2002.

A significant number of the leads generated by the TFTP have been shared with European authorities and EU Member State Governments, and more than 18,000 TFTP-derived leads have been shared through February 2016.

Q.2: What European bodies approved the Agreement?

A.2: Following the completion of negotiations, the Agreement was approved by the European Commission. The Agreement was then approved by the Council of the European Union and signed by the US and the EU on June 28, 2010. The European Parliament gave its consent to the Agreement on July 8, 2010. The Agreement entered into force on August 1, 2010.

Q.3: Have any reviews of the TFTP taken place?

A.3: Yes. In February 2011, October 2012, and April 2014, officials from the EU and US conducted a Joint Review of the implementation and effectiveness of the Agreement, pursuant to Article 13 of the Agreement. In accordance with the Agreement, the EU delegations included European Commission officials, two data protection experts from EU member state data protection authorities, and a judicial expert from Eurojust. In March 2011, December 2012, and August 2014, the European Commission issued reports prepared by the EU delegations of the Joint Review teams. Those reports are available on the European Commission's website: ec.europa.eu.

The US Government agrees with the Commission reports' joint review findings that the operation and implementation of the Agreement are consistent with the US commitment to implement the robust data protection safeguards contained in the Agreement. The US Treasury Department carefully considers the EU delegations' recommendations as it continues to implement the Agreement.

In addition, an independent person appointed by the EU conducted two reviews of the TFTP. Reports issued by the independent person in 2008 and in early 2010 concluded that the US had implemented significant and effective controls and safeguards which ensure respect for the protection of personal data. The reports also stated that TFTP leads shared with EU authorities had not only been extremely valuable in investigating terrorist attacks which have taken place in Europe over the eight years preceding the reports, but had also been instrumental in preventing a number of terrorist attacks in Europe and elsewhere.

Q.4: How does the TFTP operate?

A.4: Under the TFTP, the US Treasury Department issues administrative production orders (Requests) to the Society for Worldwide Interbank Financial Telecommunication (SWIFT), an international member-owned cooperative providing communications services to financial institutions, for narrow sets of financial messaging data transmitted between SWIFT customers which are relevant to terrorism investigations. Requests are narrowly tailored based on past or current analyses of relevant message types, geography, and perceived terrorism threats. The subsets of data transferred to the US Treasury Department pursuant to the Requests are subject to strict security measures and cannot be read or browsed, nor can they be searched, except where various elaborate safeguards (detailed below) are satisfied.

Under the Agreement, the US Treasury Department provides a copy of any Request for data to be transmitted from the EU, along with any supplemental documents, to Europol to verify whether the Request clearly identifies the data requested, is narrowly tailored, substantiates

the necessity of the data, and does not seek Single Euro Payments Area data. Once that verification occurs, Europol so notifies the data provider and the data provider transmits the data to the US Treasury Department. The US Treasury Department has coordinated closely with Europol since the entry into force of the Agreement, including by providing additional clarifying information in response to Europol inquiries.

Q.5: What are the safeguards protecting the data?

A.5: President Obama has made the protection of privacy and civil liberties a top priority. Consistent with this decision, and in accordance with past practice, the US Treasury Department has applied extraordinarily strict controls over the data to ensure data security and integrity, as well as necessary and proportionate processing of data. Safeguards in the Agreement include the following:

- Data are maintained in a physically secure, stand-alone computer network – not connected to any other data system – and subject to highly limited access rights.
- Data may be searched only for counter-terrorism purposes and not for any other type of criminal activity or for any other purpose, including counter-proliferation.
- No search may be conducted on data unless a TFTP investigator provides pre-existing information demonstrating a nexus between the subject of the search and terrorism or its financing.
- The TFTP may not be used for data mining or any other type of algorithmic or automated profiling or computer filtering.
- Detailed logs are maintained of all searches made, including the nexus to terrorism or its financing required to initiate the search.
- A select group of independent overseers, including two persons appointed by the EU, have access to and authority to review all searches of the provided data undertaken by a TFTP investigator. Independent overseers can block searches if they do not satisfy all of the safeguards.
- The EU and the US jointly review the implementation of the Agreement – with particular regard to the safeguards, controls, and reciprocity provisions set out in the Agreement – on a regular basis, and the European Commission thereafter presents a report on the review to the European Parliament and the Council.

Reports issued in 2008 and early 2010 by an independent person appointed by the EU concluded that the US had satisfied strict data protection safeguards. The 2014 report prepared by the EU delegation of the Joint Review team and adopted by the European Commission expressed the Commission's full satisfaction that the TFTP Agreement and its robust data protection safeguards are being properly implemented, and that the oversight mechanism is effective and functioning smoothly.

An external auditing firm appointed by the data provider continues to perform a separate, independent audit. The external auditors have full access to all TFTP systems and personnel.

Q.6: What redress provisions are available to EU citizens and residents?

A.6: Under the Agreement, persons may seek access to data, including a confirmation whether their data protection rights have been respected and whether improper processing of their personal data has occurred, as well as rectification, erasure, or blocking of inaccurate data. Requests for data, confirmations, or rectification may be submitted to the relevant European national data protection authority, which shall transmit the requests to the privacy officer of the US Treasury Department. After an appropriate review, the privacy officer then must: (a) inform the relevant European national data protection authority whether personal data may be disclosed to the data subject or whether data have been rectified, as appropriate; (b) confirm whether the data subject's rights have been duly respected; and (c) where access to personal data is refused based on reasonable exemptions from disclosure or rectification is refused, explain the refusal in writing and provide information on the means available for seeking administrative and judicial redress in the United States.

The Agreement further provides that any person who considers his or her personal data to have been processed improperly may seek effective administrative or judicial redress in accordance with the laws of the EU, its Member States, and the US. The US Treasury Department will treat all persons equally in the application of its administrative processes, regardless of nationality or country of residence.

All persons, regardless of nationality or country of residence, have available under US law a process for seeking judicial redress from an adverse administrative action. The Administrative Procedure Act, for example, provides a process for persons, regardless of nationality or country of residence, who have suffered harm as a result of a US Government action to seek judicial review of that action. Other examples of relevant laws providing for non-discriminatory judicial redress include the Computer Fraud and Abuse Act, which authorizes persons who suffer damage or loss by reason of a violation of the Act to maintain a civil action against the violator, including, as appropriate, a US Government official, to obtain damages or other relief, and the Freedom of Information Act, which allows persons to utilize administrative and judicial processes to seek Government information.

Q.7: What does rectification mean in the context of the TFTP?

A.7: The TFTP Agreement provides that data provided to the US Treasury Department "shall not be subject to any manipulation, alteration, or addition." Accordingly, in the unlikely event that it is notified of an error in the financial payments messaging data provided to the US Treasury Department that warranted rectification, the Treasury Department will

take appropriate steps to prevent the future use or dissemination of the erroneous data, and will annotate any existing documents produced from the erroneous data. To date, no such erroneous data have been discovered.

Q.8: How can I find out more about available redress options?

A.8: The US Treasury Department has made available on its website a document detailing the procedures for seeking redress under the Agreement (see “Redress Procedures for Seeking Access, Rectification, Erasure, or Blocking,” available at [treasury.gov/tftp](https://www.treasury.gov/tftp)). For additional information or inquiries regarding procedures for seeking access, rectification, erasure, blocking, or redress under the Agreement, you may also contact the US Department of the Treasury or your national data protection authority (“NDPA”). Contact information for each NDPA in each EU Member State can be found via the official website of the European Commission at ec.europa.eu.

Q.9: To whom should requests for access, rectification, erasure, or blocking be sent?

A.9: Appropriate requests for access, rectification, erasure, or blocking should be transmitted through express courier (or any delivery service that provides confirmation tracking numbers) by the relevant NDPA to the following address: Privacy Officer / TFTP, JBAB, Building 410 (Door 123), 250 Murray Lane SW, Washington, DC, USA 20222.

Q.10: How long are data stored under the TFTP?

A.10: The US has agreed to destroy data after five years, which is the same time period the EU uses under Directive 2005/60/EC (on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing) and Regulation (EC) No. 1781/2006 (on information on the payer accompanying transfers of funds). Leads generated for use in specific matters are retained for no longer than necessary for specific investigations or prosecutions for which they are used.

In addition, the Agreement required the EU and the US to prepare a joint report regarding the value of TFTP data, with particular emphasis on the value of data retained for multiple years and relevant information obtained from the Joint Review conducted pursuant to the Agreement. That joint report on the TFTP’s value, transmitted by the European Commission to the European Parliament and Council in November 2013, concluded: “Taking into account both the unique value of historical data and its prevalence among the TFTP leads, the reduction of the TFTP data retention period to anything less than five years would result in significant loss of insight into the funding and operations of terrorist groups.” That report is available at ec.europa.eu.

Q.11: I heard that the TFTP may be the reason my bank blocked a transaction to my account and my goods were stopped at a border crossing. Is that possible?

A.11: No. The TFTP cannot interdict or view “live” transactions as they occur; instead, it involves a narrow review of specific, terrorism-related financial transactions that already have occurred in order to further investigations of terrorist plots and activity.

Q.12: Does the US send an EU customer’s transaction data to countries outside of the EU?

A.12: The US shares counter-terrorism leads generated by the TFTP with relevant Governments for counter-terrorism purposes only. We do this consistent with UN Security Council Resolution 1373 (2001), which includes provisions stating:

- that States shall take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information;
- that States shall afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts;
- that States should find ways of intensifying and accelerating the exchange of operational information;
- that States should exchange information in accordance with international and domestic law; and
- that States should cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and to take action against perpetrators of such attacks.

The Agreement limits the transfer to third countries of EU persons’ data and authorizes such transfers only for counter-terrorism purposes and subject to a variety of additional safeguards.

Q.13: Is the US assisting the EU to develop an equivalent to the TFTP?

A.13: If the EU decides to establish an EU system, the US has agreed to provide assistance and advice to contribute to the system’s effective establishment. US and EU authorities would cooperate to ensure that the US and EU systems are complementary and efficient in a manner that further enhances citizens’ security.

