EUROPEAN
COMMISSION

Brussels, 27.11.2013
SWD(2013) 489 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

A Communication from the European Commission to the European Parliament and the Council on a European Terrorist Financing System (TFTS)

{COM(2013) 842 final}
{SWD(2013) 488 final}

COMMISSION STAFF WORKING PAPER

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

A Communication from the European Commission to the European Parliament and the Council on a European Terrorist Financing Tracking System (TFTS)

1. INTRODUCTION

In 2010, when the EU concluded the Agreement between the European Union and the United States on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purpose of the Terrorist Financing Tracking Program (EU-US TFTP Agreement), the Commission was asked by the Council and the European Parliament to look for a similar system which would enable the extraction of such data on EU territory. The EU-US TFTP Agreement refers to such a European system in one of its articles by stating that the European Commission would carry out a study into the introduction of an equivalent system for the EU.

Given the legal and technical complexity of the issue it stake and its sensitivity with regard to its impacts on fundamental rights, in particular personal data protection, the Commission decided to publish in July 2011 a Communication with various options to show what forms the establishment of such a system could have.

Subsequent discussions and feedback did not reveal a clear preference by Member States or by the European Parliament for any of the options. Therefore the Commission decided to look at all of them in this Impact Assessment and to elaborate on these options by developing different sub-options.

Since the Commission was called upon to propose a framework for an EU Terrorist Financing Tracking System (TFTS), the economic situation in Member States and in the EU has

changed and Member States have become increasingly aware of the possibility of benefiting from data exchange based on the EU US TFTP Agreement, due to the reciprocity clauses contained in it. These developments and factors were taken into account when comparing the options for the introduction a new system with the option of maintaining the status quo, as this status quo has changed since 2010.

2. PROBLEM DEFINITION

The transnational nature of Terrorist Financing make detection of and acting against the funding of terrorism very challenging

According to EUROPOL's latest TE-SAT Report 2012, Member States continue to face to a serious threat from terrorism, be it religiously inspired/Islamist, ethno-nationalist and separatist, left– or right wing or anarchist terrorism. In order to deprive terrorists of their capacity to engage in terrorist activity it has been a core component of the EU's counter terrorism strategy to prevent terrorists and entities from collecting, moving and gaining access to funds. Countering terrorist financing means preventing financial support of terrorism or of those who encourage, plan, or engage in terrorism.

Terrorist activities are very often transnational in character. Not only do they encompass activities that are planned in one country and carried out in another but they involve fund raising activities and transfers which cross borders. Transnational activities allow terrorists to hide the ways they move their money, its origin and its purpose. Because of its transnational nature, detecting and stopping the financing of terrorism is extremely challenging. International cooperation in this field is therefore of paramount importance. This is why the EU agreed to work together with the United States in this field, as demonstrated by the EU US-TFTP agreement in particular.

In addition to a number of legislative instruments, there are also a number of international and EU bodies which are actively involved in the fight against terrorist financing and which promote international or EU co-operation. These bodies are the Financial Action Task Force on Money Laundering and Terrorist Financing (FATF), the Committee on the Prevention of Money Laundering and Terrorist Financing, the EU Financial Intelligence Units (FIU) Platform, Eurojust and Europol. To enhance co-operation among EU Member States there are

a number of legislative instruments in place, such as a Decision on co-operation amongst EU Financial Intelligence Units.

Existing instruments/ measures are inadequate for tracking the financial trail of terrorists

Even though co-operation amongst EU Member States in this field is constantly improving, including co-operation based on the introduction of new legal instruments such as the European Evidence Warrant, information exchange on financial data is limited. Mutual legal assistance instruments or co-operation between EU Financial Intelligence Units are not capable of and are not aimed at mapping and profiling a suspect, quickly uncovering all existing accounts and related financial transactions of a suspect (and those of companies and other organisations on his or her name) of a person, across the world, going back several years. Apart from the TFTP there is at present no instrument that can generate information on the suspect at the very start of an investigation within a very short time period, enabling investigators to focus on certain categories of financial transactions, certain countries and/or a certain time period, to establish a clear timeline with regard to a suspect's movements. The TFTP is, however, a tool which is exclusively operated by the US which means that it is primarily used in view of US security needs.

The Problem Drivers

1. **The current mechanism in place to analyse financial messaging data is led by a third country, thus not fully representing EU's specific interests.**

In the EU, the terrorist threat comes mainly from separatist, religiously inspired, left- and right-wing and anarchist terrorists. These threats appear to be 'cyclical' in terms of their intensity and the risk they represent and are, to some extent, quite different from the threat to the US. The threat in the latter mainly comes from Islamist terrorism, which does not have a presence in the US itself, or has only a limited presence.

The primary purpose of the TFTP is investigating terrorist activity linked to the threat as perceived by the US. Nevertheless the Member States have increasingly started to use the reciprocity clauses in the Agreement to benefit from the data exchanges with the US. Hence this problem driver is changing over time and its importance is decreasing with Member

States gaining more experience with the use of the Agreement and the TFTP in order to address threats to the EU.

2. **The current mechanism in place to analyse financial messaging data only covers one financial messaging provider and one type of message**

Given that it is a US programme with a global focus, at present, only FIN messages (Financial Institution Transfer messages) transferred through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network are included in the TFTP. FIN messages are a SWIFT-created message type by which financial information is transmitted from one financial institution to another. However, aside from SWIFT transfers, there a number of other important electronic payments transfer systems and various other providers in the market, such as Automated Clearing Houses and e-money transfers. These are currently not checked by the TFTP and could consequently be used by terrorists or entities linked to terrorism to transfer their funds, without being subject to checks.

3. **The current mechanism in place to analyse financial messaging data raises concerns as to the protection of privacy and personal data of European citizens**

Most criticism concerns the TFTP's alleged inconformity with the right to respect for private and family life (Article 7 of the Charter of Fundamental Rights) and the right to the protection of personal data (Article 8 of the Charter of Fundamental Rights and Article 16 of the TFEU), as well as with the obligations under the Data Protection Directive (Directive 95/46/EC). Doubts have been expressed over the necessity and proportionality of transferring data on EU citizens to a third country and over the verification and authorisation processes allowing for the transfer of such data.

The two joint reviews on the application of the EU US Agreement on the TFTP verified proper implementation of the comprehensive safeguards included in the Agreement, including those related to the protection of personal data. The practical and more experienced application of the Agreement by the EU and US has put this problem driver into context, showing that the original concerns have been addressed by the effective set of safeguards.

4. **Besides the EU US TFTP Agreement, there is insufficient technical and legal capability within the EU and in Member States to establish financial linkages to trace and map terrorist networks**

At the level of the EU, there is no equivalent separate system in place which would disclose financial linkages to trace and map terrorist networks. The existing legislative and operational instruments which have been set up at the level of the EU and Member States or in which the EU and Member States participate (like FIU platform) do not, cannot and have not been created to offer the same advantages as the TFTP in terms of speed, efficiency and effectiveness. Pursuant to the preventive system based on the 3rd Anti-Money Laundering Directive, for example, Financial Intelligence Units analyse financial transactions on a case by case basis following suspicious transaction reports by obliged entities such as financial institutions. The EU freezing system related to terrorist funds requires a formal list of persons and entities related to terrorism agreed by the Council in order to prevent financial transactions of those listed. But there is no system in place that uses data which would make it able to show a complete pattern of financial "behaviour" and connections of a person or organisation suspected of terrorism or financing terrorism.

The baseline scenario

Under the baseline scenario, no EU TFTS system would be created at this stage. The EU-US TFTP Agreement would continue to exist and to be applied. There would be just one Designated Provider obliged to disclose relevant financial data and only its FIN messages would be covered. Member States as well as Europol and Eurojust would continue to be able to use the reciprocity clause included in the EU-US TFTP Agreement. This clause enables EU authorities to obtain directly relevant financial data from the U.S. Treasury which helps them to fight terrorism and its financing more efficiently in the EU. In addition, the U.S. Treasury would continue sending reports on possible terrorist threats to Member States and Europol without a specific request based on Article 9 of the EU-US TFTP Agreement. The current level of personal data protection would be maintained while, at the same time, also not increasing the amount of data collected. The two joint reviews of the TFTP agreement have verified the proper functioning of the TFTP and of the robust control measures which are in

place to ensure that safeguards, including those on personal data protection, are duly respected.

The cost of establishment of a new system, including both the initial investment and annual running cost, would be avoided. There would be no additional exposure of personal data and no varied level of risk to be mitigated (unlike any of the options for the EU system).

3. OBJECTIVES AND OPTIONS

Objectives

Terrorist offences cause severe harm to victims, inflict economic damage on a large scale and undermine the sense of security without which persons cannot exercise their freedom and individual rights effectively. Therefore the overarching and principal objective of an EU TFTS would be to cut off terrorists' access to funding and to track financial transactions linked to terrorism, in order to enhance security in the EU.

To achieve this goal, the Commission has identified five specific objectives, namely to ensure that the system is tailored to respond to EU intelligence requirements using EU threat assessments, to maintain effective cooperation with the US and other third countries in the fight against terrorism, to ensure that the analysis of financial messaging data covers the most relevant service provider(s) and message type(s), to ensure full protection of the rights to privacy and data protection of European citizens when processing financial messaging data, and to increase the EU and Member State access to and analyses of financial messaging data and their capacity to identify links between individuals/ groups involved in terrorism or its financing. Operational objectives linked to the problem drivers complete the framework in which the various options were considered.

Options

In terms of policy options, the Impact Assessment identifies four levels of options of which the first two relate to the structure of a tracking system, the third to the purpose, and the fourth to the scope: “No EU TFTS options”, “EU TFTS with various sub options for the structure”, “options for the purpose of an EU TFTS” and “options for the scope of an EU TFTS”. In each level a number of sub-options are listed and further described. Four sub-options have been discarded as they would clearly worsen the current situation, would depend on the agreement

of a third country or would have an significant negative impact on Member States' budgets. The remaining options are the following:

-the baseline scenario – status quo

- three hybrid systems for the creation of an EU TFTS, ranging from a very high to a very low level of EU involvement:

1. The EU TFTS coordination and analytical service model envisages the creation of an EU central TFTS unit with most of the tasks and functions implemented at EU level. However, Member States could also do their own searches via designated national TFTS experts based in the same location as the EU TFTS unit.

2. The EU TFTS extraction service model would establish an EU central TFTS unit with the task of issuing requests for raw data to the designated provider(s). Member States would have the right to request searches to be run on their behalf.

3. The FIU coordination model would involve the establishment of an ad-hoc EU-level authority, made up of all Member States' FIUs with a division of tasks between this central unit and the national FIUs.

-two retention/ extraction systems:

1. The first model would be a retention system asking the Designated Provider(s) to retain the data on its/their server for a certain period of time.

2. The second option would be like the previous one but with the creation of a search facility on the premises of the Designated Provider(s).

-two options regarding the purpose of an EU TFTS, one limiting it to combatting terrorism, the second one adding serious organised crime to it.

-two options regarding the scope with the first one limiting it to the current Designated Provider SWIFT and the second encompassing multiple Designated Providers.

4. ASSESSMENT OF IMPACTS

The economic impacts of the options have to rely on estimates and assumptions. The possible economic benefits are not easy to measure, even though the European Commission is aware

that in other contexts, such as in relation to health issues, this might be undertaken by applying the "Quality adjusted life year" methodology. In the context of terrorism, however, it appears impossible and disproportionate to try to weigh by figures the value of human lives that could be saved by preventing terrorist attacks. It is also not possible to predict in detail the economic benefits of such a system helping to prevent terrorist activity and the damages it causes to the economy or state-owned or private property as the extent of attacks and the damages caused depend on a great number of unpredictable variables. Likewise, the social and psychological impact of terrorist attacks is difficult to quantify.

In addition, it needs to be recalled that the present mechanism is meant to be a security policy instrument. Data available in this context is highly confidential in order to prevent those targeted by the instrument from being in a position to circumvent it or adapt their criminal and terrorist behaviour so that the system would not be able to detect them. This limits the ability to provide the same detail when identifying, assessing and comparing impacts as one may be used to from similar exercises in other policy fields for this specific Impact Assessment the possibility to. Finally, a great amount of information used for the analysis carried out stems from a third country source (US) that has practical experience with a similar system to fight terrorism and its financing. This information is to a large extent classified as it is essential for the security situation in this country (US). Even if it cannot be made public in this assessment, the European Commission was able to consider important parts of it in its analysis of the issue at stake.

Regarding the costs expected for the various options a detailed calculation is annexed to the Impact Assessment. Apart from the economic impact, the effectiveness of the various options (i.e., their ability to achieve the objectives), is another important category of impact. In addition, for each option the social and human rights related impacts were assessed as well as the political impact which included the effect on relations with third countries, in particular the US. In terms of other impacts the impact assessment gives detailed consideration to how practicable the envisaged measure would be and to whether the measure would be acceptable to the various stakeholders and the public.

5. CONCLUSION

After identifying and analysing the possible options regarding the establishment of an EU TFTS and assessing the impacts of the different options, the Commission considers that at present the preferred and the most proportionate option is to maintain the status quo. Any EU system would be data intrusive and would therefore require robust data protection guarantees and safeguards to be put in place. It would be costly and also technically and operationally demanding to set up and maintain.

The baseline scenario has evolved over time. Member States are increasingly making use of the reciprocity clauses and benefit from the data transfer to the US to enhance security in the EU and to prevent terrorism. This shows that the principal objective identified for the establishment of an EU TFTS is in the state of being addressed by an already existing system, the EU-US TFTP Agreement. In view of these developments and at this stage, the Commission does not regard as justified the establishment of a new terrorist financing tracking system with all its demonstrated implications such as further personal data collection and extra costs for its creation and maintenance.