SUPPORTING STATEMENT
U.S. Department of Commerce
International Trade Administration
Information for Self-Certification under FAQ 6 of the United States (U.S.) - European Union (EU) Safe Harbor Framework and United States (U.S.) - Switzerland (Swiss) Safe Harbor Framework
OMB Control No. 0625-0239

A. JUSTIFICATION

This is a request for approval of an existing information collection revision.

1. Explain the circumstances that make the collection of information necessary.

The following concerns the Safe Harbor self-certification form that U.S. organizations complete and submit to the U.S. Department of Commerce in order to self-certify their compliance with one or both of the Safe Harbor Frameworks. The form presently being used is an approved information collection; however, the version of the form for which an extension is being sought includes several revisions. The revised form features additional guidance (i.e., helpful reminders and explanations about how to provide appropriate responses in fields that have been part of the form ever since it was first approved), but does not entail any additional burden in terms of cost or time required complete.

The European Union Directive on Data Protection (hereinafter EU Directive), which went into effect in October 1998, restricts transfers of personal data from EU Member States to countries that are not deemed by the EU to provide "adequate" data protection (i.e., privacy protection). Although the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU. In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the EU Directive, the U.S. Department of Commerce (DOC) in consultation with the European Commission developed a "Safe Harbor" framework (i.e., the U.S.-EU Safe Harbor Framework) to ensure that personal data flows to the United States could continue. The DOC consulted with U.S. organizations affected by the EU Directive, as well as interested non-government organizations during the development of the U.S.-EU Safe Harbor Framework.

On July 26, 2000, the European Commission issued a decision – in accordance with Article 25.6 of the EU Directive – finding that for all of the activities falling within the scope of the EU Directive, the Safe Harbor Privacy Principles, implemented in accordance with the guidance provided by the Frequently Asked Questions issued by the DOC (i.e., collectively the U.S.-EU Safe Harbor Framework) are considered to ensure an "adequate" level of protection for personal data transferred from the EU to organizations established in the United States. The EU Member States implemented the European Commission's decision within 90 days; therefore, the "U.S.-EU Safe Harbor" became operational on November 1, 2000. The European Economic Area

(EEA) also has recognized the U.S.-EU Safe Harbor Framework as providing "adequate" data protection.

The Swiss Federal Act on Data Protection (hereinafter "Swiss FADP"), which went into effect in July 1993, followed by important modifications in January 2008, restricts transfers of personal data from Switzerland. Although the United States and Switzerland share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by Switzerland. In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the Swiss FADP, the DOC in consultation with the Federal Data Protection and Information Commissioner of Switzerland (hereinafter "Swiss FDPIC") developed a "Safe Harbor" framework (i.e., the "U.S.-Swiss Safe Harbor Framework") to ensure that personal data flows to the United States could continue. The DOC consulted with U.S. organizations affected by the Swiss FADP, as well as interested non-government organizations during the development of the U.S.-Swiss Safe Harbor Framework. The "U.S.-Swiss Safe Harbor" became operational in 2009.

The complete set of U.S.-EU and U.S.-Swiss Safe Harbor documents and additional guidance materials may be found at http://export.gov/safeharbor.

For purposes of the Safe Harbor Frameworks, "personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the EU Directive, received by a U.S. organization from the European Union and/or Switzerland, and recorded in any form. "Personal data" is defined in the EU Directive as "…any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". The scope of the EU Directive is rather broad. It applies to all "processing of data", which is defined as "…any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

Each month, the DOC receives approximately 65-70 new applications (i.e. initial self-certification submissions) to participate in the Safe Harbor program(s), a majority of which will ultimately be finalized (i.e., those organizations will be assured of Safe Harbor benefits, so long as they maintain their certification status through annual reaffirmations, and otherwise continue to comply with the requirements of the Safe Harbor program(s)). It is very difficult to estimate how many organizations will ultimately participate in the Safe Harbor program(s).

Safe Harbor Benefits: The Safe Harbor Frameworks provide a number of important benefits, especially predictability and continuity, to U.S. organizations that receive personal data for processing from the EU/EEA and/or Switzerland. All 28 EU Member States, and by extension all EEA Member States, are bound by the European Commission's finding of "adequacy". The Safe Harbor eliminates the need for prior approval to begin data transfers or makes approval from the national data protection authority automatic. The Safe Harbor Frameworks offer a simpler and more cost-effective means of complying with the relevant requirements of the EU

Directive and Swiss FADP, which should particularly benefit small and medium enterprises.

Which organizations can join?: Any organization that is subject to the enforcement authority of either: (a) the Federal Trade Commission (hereinafter "FTC") under Section 5 of the Federal Trade Commission Act; or (b) the Department of Transportation if an air common carrier or ticketing agent. Other regulatory agencies may be added over time.

How does an organization join?: The decision by an organization to self-certify its compliance with one or both of the Safe Harbor Frameworks is entirely voluntary; however, once made, the organization must comply with the requirements of the relevant Safe Harbor Framework and publicly declare that it does so. To be assured of Safe Harbor benefits, an organization must reaffirm its self-certification annually (Form ITA-4149P) to the DOC in accordance with the requirements specified in the Framework(s) and guidance provided by the DOC. An organization's self-certification of compliance with one or both of the Safe Harbor Frameworks, and the appearance of the organization on the relevant Safe Harbor List(s) pursuant to the self-certification, constitute an enforceable representation to the DOC and the public that it adheres to a privacy policy that complies with the relevant Safe Harbor Framework(s).

2. Explain how, by whom, how frequently, and for what purpose the information will be used. If the information collected will be disseminated to the public or used to support information that will be disseminated to the public, then explain how the collection complies with all applicable Information Quality Guidelines.

The DOC maintains two public lists - the "U.S.-EU Safe Harbor List" and the "U.S.-Swiss Safe Harbor List" - of U.S. organizations that have self-certified their compliance with the U.S.-EU Safe Harbor Framework and/or the U.S.-Swiss Safe Harbor Framework. The DOC also provides guidance on the substantive requirements and logistical steps needed to participate in the Safe Harbor programs and appear on the respective lists. Both of the Safe Harbor Lists are made available to the public on the DOC's Safe Harbor website.

Organizations that have self-certified their compliance with one or both of the Safe Harbor Frameworks, appear on the relevant Safe Harbor Lists, and have not allowed their certification status to lapse are presumed to provide "adequate" data protection in accordance with the EU Directive and/or the Swiss FADP and therefore are not required to provide further documentation to European officials on this point. The Safe Harbor Lists are used by EU and Swiss citizens and organizations to determine whether further information and/or contracts will be required for a U.S. organization to receive personally identifiable information. The Safe Harbor Lists are necessary to make the Safe Harbor Frameworks operational, and were a key demand of the European Commission and the Swiss FDPIC in agreeing that compliance with the Safe Harbor Frameworks provide "adequate" privacy protection.

The Safe Harbor Lists, which are updated on a regular basis, will be used by U.S. and European authorities to determine whether an organization has self-certified its compliance with one or both Safe Harbor Frameworks, especially when a complaint has been lodged against a given U.S.

organization. For example, the Lists will be used by the EU and Swiss data protection authorities to determine whether an organization is providing "adequate" data protection, and whether it has agreed to cooperate and comply with such data protection authorities. Any public misrepresentation concerning an organization's participation in the Safe Harbor or compliance with one or both of the Safe Harbor Frameworks may be actionable by the FTC or other relevant government body (e.g., the Department of Transportation). For example, organizations that self-certify their compliance with one or both of the Safe Harbor Frameworks, but fail to comply with the Safe Harbor Privacy Principles or otherwise misrepresent their certification status may be subject to enforcement by the FTC. Under the Federal Trade Commission Act, such conduct could be considered deceptive and actionable. The FTC has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to $16,000 per day for violations of those orders. In addition, misrepresentations to the DOC (or its designee) may be actionable under the False Statements Act (18 U.S.C. Section 1601).

Required Information: The following information is required under Frequently Asked Question (FAQ) 6 of the Safe Harbor Frameworks. This information is:

1. *Date on which an organization's original self-certification of compliance with the Safe Harbor Framework(s) was finalized (i.e., date on which its participation in the Safe Harbor program(s) commenced) and date by which it must recertify (i.e., date by which it must submit its annual reaffirmation of compliance with the Safe Harbor Framework(s)).* This information allows the DOC to inform an organization (i.e., via e-mail) that it must reaffirm its self-certification and when it must do so. The relevant date also informs the public whether or not the organization has recertified as is required to maintain its certification status and is therefore entitled to Safe Harbor benefits.

2. *Organization Name and address [street and number, city, state, zip code, website].* This information identifies the organization that is self-certifying its compliance with the Safe Harbor Framework(s).

3. *Organization Contact [office, name, title, office, phone number, and e-mail address]* handling complaints concerning the organization's privacy practices, access requests, and other inquiries concerning the organization's compliance with the Safe Harbor Framework(s). The DOC will also typically send correspondence concerning the organization's certification status, including recertification reminders, to the individual or office listed as the "Organization Contact".

4. *Corporate Officer [name, title, phone number, and e-mail address]* certifying the organization's adherence to the Safe Harbor Framework(s). This information will be used by the government if an individual's privacy-related complaint is not handled appropriately. Individuals submitting information for self-certification are required to give their names and titles and to attest that they have the authority to submit the self-certification on behalf of their respective organizations.

5. *Description of the organization's activities with respect to personal information received from the EU/EEA and/or Switzerland*. This information provides individuals with a brief summary of what, why, and when such personal information is received.

6. *Effective date of the organization's privacy policy and the location where the privacy policy statement is publicly accessible.* This information provides individuals, European organizations, and government bodies with the date when the privacy policy entered into effect and where it can be reviewed.

7. *Statutory body.* In order to be eligible to participate in the Safe Harbor program(s), an organization must fall under the jurisdiction of either the FTC or the Department of Transportation. This information identifies the body that has jurisdiction to hear claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing the organization's privacy practices.

8. *Any privacy programs that an organization is a member of*. Organizations do not have to be in a privacy program in order to join the Safe Harbor. However, an organization may sign up to a self-regulatory privacy program that complies with the Safe Harbor's requirements. This information provides individuals and governments with what self-regulatory program a complaint should go to if an organization is not living up to its commitments.

9. *Verification method [i.e., in-house / self-assessment; or third party / external assessment]*. This information identifies how the organization verifies, at least annually, that its privacy practices comply with the requirements of the Safe Harbor Framework(s).

10. *Independent Recourse Mechanism(s) [i.e., private sector developed dispute resolution mechanism that incorporates the Safe Harbor Framework(s); and/or the EU and/or Swiss data protection authorities]*. This information identifies which third party dispute resolution mechanism is available to investigate unresolved individual privacy-related complaints, when the organization could not or would not address an individual's complaint in a timely or otherwise satisfactory manner.

11. *Personal data coverage [e.g., organization, customer / client, visitor, clinical trial, etc.]*. The organization must identify, at least generally, what type of data it seeks to cover under its self-certification. The organization must specify if it seeks to cover manually processed data under its self-certification, as that category of data is not automatically covered.

12. *Organization human resources data coverage*. The organization must confirm whether or not it seeks to cover 'organization human resources data' (i.e., personal information concerning its own employees, past or present, collected in

the context of the employment relationship) under its self-certification. In addition, if the organization does confirm that it intends to cover such data, then it must also confirm that it agrees to cooperate and comply with the appropriate European data protection authorities (i.e., in the investigation and resolution of complaints concerning its handling of such data).

All information listed above is required for the organization to self-certify under the Safe Harbor program(s). Enforcement is predicated on the representations made by the organization through self-certification that it will adhere to the Safe Harbor Framework(s) when handling personal information transferred from Europe.

Optional Information: The DOC also requests that organizations provide the following additional information:

1. *The countries [i.e., the 28 EU Member States, 3 EEA Member States, and/or Switzerland] from which the organization receives personal information.* This information could be used by European organizations looking for Safe Harbor participants active in particular countries.

2. *Industry sector.* This information could be used by European organizations looking for Safe Harbor participants from a particular industry sector.

3. *Level of sales and number of employees.* This information, which will not be disseminated to the public, will allow the DOC to determine what proportion of the participants are small and medium enterprises (i.e., whether further outreach is necessary).

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological techniques or other forms of information technology.

The DOC offers U.S. organizations the opportunity to provide the self-certification described above via the DOC's Safe Harbor website: http://export.gov/safeharbor. Organizations interested in participating in the Safe Harbor programs are strongly encouraged to make their initial self-certification, as well as annual recertification submissions, including payment of the relevant processing fee, online via the Safe Harbor website. The Safe Harbor website also provides organizations already in the program with direct access to their records thereby enabling them to update the information provided therein throughout the year. The electronic method is strongly encouraged, as it is expressly designed to process submissions in a timely and accurate manner. An organization cannot make initial self-certification, as well as annual recertification submissions, or other updates to an existing submission via the DOC's Safe Harbor website unless it uses that organization's username of record and present password. At present, an overwhelming majority of organizations making initial self-certification or annual recertification submissions do so electronically via the DOC's Safe Harbor website.

4. Describe efforts to identify duplication.

There is no duplication. The Safe Harbor Frameworks are unique methods for handling personal data flows between the EU/EEA and/or Switzerland, and the United States. Under the terms of the DOC's agreement with the European Commission and the Swiss FDPIC, the DOC has the sole responsibility for collecting and making publicly available the lists of organizations that self-certify their compliance with the Safe Harbor Frameworks.

5. If the collection of information involves small businesses or other small entities, describe the methods used to minimize burden.

The Safe Harbor Frameworks provide a number of important benefits, especially predictability and continuity, to U.S. organizations of all sizes that receive personal data for processing from the EU/EEA and/or Switzerland. All 28 EU Member States, and by extension all EEA Member States, are bound by the European Commission's finding of "adequacy". The Safe Harbor eliminates the need for prior approval to begin data transfers or makes approval from the national data protection authority automatic. The Safe Harbor Frameworks offer a simpler and more cost-effective means of complying with the relevant requirements of the EU Directive and Swiss FADP, which should particularly benefit small and medium enterprises.

6. Describe the consequences to the Federal program or policy activities if the collection is not conducted or is conducted less frequently.

Removing or reducing the collection of information associated with self-certification under the Safe Harbor Frameworks would prevent the U.S. Government from implementing the agreements reached separately between the European Commission and the DOC, and the Swiss FDPIC and the DOC. As a result, the flow of personally identifiable data between Europe and the United States could be seriously disrupted. Alternatives to the Safe Harbor Frameworks that exist under the EU Directive are more time-consuming, costly, and particularly burdensome to small and medium sized enterprises.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with OMB guidelines.

Not Applicable.

8. Provide information of the PRA Federal Register Notice that solicited public comments on the information collection prior to this submission. Summarize the public comments received in response to that notice and describe the actions taken by the agency in response to those comments. Describe the efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of

instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

The Federal Register Notice requesting public comments was published on April 11, 2014 (Volume 79, Number 70, pages 20169-20171). This announcement did not generate any comments from the public.

9. Explain any decisions to provide payments or gifts to respondents, other than remuneration of contractors or grantees.

Not Applicable.

10. Describe any assurance of confidentiality provided to respondents and the basis for assurance in statute, regulation, or agency policy.

No assurance of confidentiality is given. With the exception of the information concerning level of sales and number of employees, the information provided by the respondents is public information. The respondents, who volunteer the information, know in advance that the information will be made publicly available on the DOC's Safe Harbor website consistent with DOC guidelines and program instructions.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.

There are no questions that ask respondents to provide sensitive personal data. The data provided is corporate information relating to an organization's business activities in the EU/EEA and/or Switzerland related to receipt of personal data of EU/EEA and/or Swiss citizens or employees.

12. Provide an estimate in hours of the burden of the collection of information.

Type of Response	Response Time	No. of Respondents	No. of Responses (i.e., self-certification submissions)	Total Hours
Completion and submission of initial self-certification via DOC's Safe Harbor website	40 minutes	780	780	520

Cost to respondent per response: Response Time (40 minutes) x Average Salary ($35.00/hour) = $23.33

Total cost: Total Hours (520 hours) x Average Salary ($35.00/hour) = $18,200.00

Note: As to the response time, 40 minutes is the estimated time it takes to complete the self-certification form and submit it online via the Safe Harbor website. There are essentially two types of respondents: (1) those that are self-certifying for the first time; and (2) those that are recertifying on or before the anniversary of their original self-certification, which must be renewed annually. The same form is used for both types of respondents, as those recertifying either update what was previously submitted or simply confirm that what was previously submitted remains accurate. In short, the same respondents are not asked to fill out multiple forms and pay multiple fees at the same time (i.e., the relevant burden for a given respondent would only fall once a year).

13. Provide an estimate of the total annual cost burden to the respondents or record-keepers resulting from the collection (excluding the value of the burden hours in Question 12 above).

Cost to respondent per response: Initial Self-Certification Processing Fee = $200.00

Total cost: No. of Responses / initial self-certification submissions (780) x Initial Self-Certification Processing Fee ($200.00) = $156,000.00

Note: Cost to respondent per response: Recertification Processing Fee = $100.00

14. Provide estimates of annualized cost to the Federal government.

Type of Response	Response Time	No. of Respondents	No. of Responses	Total Hours
Review and processing of initial self-certification submission	30 minutes	780	780	390

Cost to Federal Government per response: Response Time (30 minutes) x Average Salary ($35.00/hour) = $17.50

Total cost to Federal Government: Total Hours (390 hours) x Average Salary ($35.00/hour) = $13,650.00

15. Explain the reasons for any program changes or adjustments.

The adjusted figures provided in the responses to #12 and #14 reflect a rise in the number of "responses" (i.e., self-certification submissions) received, reviewed, and processed each year.

The references to the U.S.-Swiss Safe Harbor Framework (i.e., in addition to references to the U.S.-EU Safe Harbor Framework that appeared in material submitted as part of previous clearance renewals) in this supporting statement and other material submitted this year as part of the OMB clearance renewal process clarifies that the Safe Harbor self-certification form has been used since 2009 to collect information relating to both Safe Harbor Frameworks. As was stated above in this supporting statement, the U.S.-EU Safe Harbor Framework came into existence in 2000, whereas the U.S.-Swiss Safe Harbor Framework came into existence in 2009 (i.e., between 2000 and 2009 the form would have only collected information regarding the U.S.-EU Safe Harbor Framework; whereas 2009 onwards the form has been used to collect information regarding both Safe Harbor Frameworks).

16. For collections whose results will be published, outline the plans for tabulation and publication.

Much of the information collected from respondents will ultimately be made public in relevant records that appear on the public Safe Harbor Lists, which the DOC maintains (i.e., for the reasons discussed elsewhere in this supporting statement) on its Safe Harbor website.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons why display would be inappropriate.

Not Applicable.

18. Explain each exception to the certification statement.

None.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

No statistical methodology employed.