SUPPORTING STATEMENT
U.S. Department of Commerce
International Trade Administration
SELF-CERTIFICATION UNDER FAQ 6 OF THE UNITED STATES – EUROPEAN UNION SAFE HARBOR PRIVACY FRAMEWORK
OMB Control No. 0625-0239

A. JUSTIFICATION

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

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

In response to the European Union Directive on Data Protection that restricts transfers of personal information from Europe to countries whose privacy practices are not deemed "adequate," the U.S. Department of Commerce developed a "Safe Harbor" framework that allows U.S. organizations to satisfy the European Directive's requirements and ensure that personal data flows to the United States are not interrupted. In this process, the DOC consulted extensively with U.S. organizations affected by the European Directive and interested non-government organizations. On July 26, 2000, the European Commission issued its decision in accordance with Article 25.6 of the Directive that the Safe Harbor Privacy Principles provided adequate privacy protection. The Safe Harbor framework bridges the differences between the European Union (EU) and U.S. approaches to privacy protection. The complete set of Safe Harbor documents and additional guidance materials may be found at http://export.gov/safeharbor.

Once the European Commission deemed the Safe Harbor "adequate" on July 26, 2000, the Department of Commerce began working on the mechanisms that are necessary to put this accord into effect. The Safe Harbor became operational on November 1, 2000. The Department of Commerce created a list for U.S. organizations to sign up to the Safe Harbor and provided guidance on the mechanics of signing up to this list. As of December 10, 2010, 2,415 U.S. organizations have placed themselves on the Safe Harbor List, located at on the website above.

We anticipate that about 40-45 new organizations a month will sign up. The total number of organizations on the Safe Harbor List should rise to about 3,000 in the next year. It is very difficult to determine exactly how many organizations will ultimately sign up. It is important to note that organizations must annually reaffirm their adherence to the Safe Harbor. Organizations that have voluntarily signed up to this list are deemed "adequate" under the Directive and, in most cases, do not have to provide further documentation to European officials.

Safe Harbor Benefits: The Safe Harbor provides a number of important benefits to U.S. firms. Most importantly, it provides predictability and continuity for U.S. organizations that receive personal information from the European Union. Personally identifiable information is defined as any that can be identified to a specific person, for example an employee's name and extension would be considered personally identifiable information. All 27 member countries are bound by

the European Commission's finding of "adequacy". Also, Norway, Iceland, and Liechtenstein are not part of the European Union but have agreed to be bound by the adequacy finding. The Safe Harbor also eliminates the need for prior approval to begin data transfers, or makes approval from the appropriate EU member countries automatic. The Safe Harbor principles offer a simpler and cheaper means of complying with the adequacy requirements of the Directive, which should particularly benefit small and medium enterprises.

What organizations can join?: Any organization that is subject to the enforcement authority of the Federal Trade Commission under Section 5 of the Federal Trade Commission Act or the Department of Transportation. Other regulatory agencies may be added over time.

How does an organization join?: The decision to enter the Safe Harbor is entirely voluntary. Organizations that decide to participate in the Safe Harbor must comply with its requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization needs to reaffirm its self-certification annually to the Department of Commerce that it agrees to adhere to the Safe Harbor's requirements, which includes elements such as notice, choice, access, data integrity, security and enforcement.

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 Safe Harbor List will be used by EU organizations to determine whether further information and contracts will be needed for a U.S. organization to receive personally identifiable information. This list is necessary to make the Safe Harbor accord operational, and was a key demand of the Europeans in agreeing that the Principles provide "adequate" privacy protection.

This list will be used by the European Data Protection Authorities to determine whether a company is providing "adequate" protection, and whether a company has requested to cooperate with the Data Protection Authority. This list will be accessed when there is a complaint logged in the EU against a U.S. organization. It will be used by the Federal Trade Commission and the Department of Transportation to determine whether a company is part of the Safe Harbor. This will be accessed if a company is practicing "unfair and deceptive" practices and has misrepresented itself to the public. It will be used by the Department of Commerce and the European Commission to determine if organizations are signing up to the list. This list is updated on a regular basis.

The Department of Commerce maintains a list of all organizations that file self-certification letters.

Required Information: The following information is required under Frequently Asked Question (FAQ) 6 of the Safe Harbor Privacy Principles. This information has been deemed necessary by the Safe Harbor Privacy Framework that was agreed with the European Commission and will be used by companies in Europe transferring personal information to the

United States, as well as individuals with a privacy complaint and government officials handling such complaints. This information is:

1. *Date the organization signed up and date they will need to recertify that they are current.* This information allows the Department of Commerce to send a letter informing the organization that it needs to reaffirm its self-certification. It also informs the public whether or not the organization is in compliance with the self-certification requirements.

2. *Organization name, address [street and number, city, state, zip code, website].* This Information identifies the organization that is self-certifying its compliance with the Safe Harbor Privacy Principles.

3. *Effective date of privacy policy and location of privacy policy for public viewing.* This information provides the individual, European organizations, and government bodies with the exact date of when the policies are going to go into effect and where they can find them so that all parties are informed.

4. *Statutory body.* Currently, in order to be eligible for the Safe Harbor, an organization must fall under the jurisdiction of either the U.S. Federal Trade Commission or the U.S. Department of Transportation. An organization may not self-certify if it does not fall within the jurisdiction of one of these two enforcement bodies. This information informs individuals and governments which enforcement body a complaint should go to if an organization is not living up to its commitments.

5. *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.

6. *Method of verification.* [a) In house self-assessment, or b) Outside assessor]. This provides the public with information about how privacy practices are being verified and what organization to go to get further information in a case a complaint arises.

7. *Independent Recourse Mechanism.* This gives information to the individual about where to bring a complaint if the organization does not initially respond.

8. *Contact office [name, title, office, phone number, and e-*mail*]* for handling inquiries and complaints. Individuals use this information in the first instance to make a complaint about an organization's privacy practices.

9. *Corporate officer self-certifying [name, title, office, phone number and e-mail].* This information will be used by the public in case of a privacy complaint and by the government if the individual's privacy complaint is not appropriately handled. 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. This information is needed to ensure that the individual can make the commitment on behalf of the company to adhere to the Safe Harbor. .

All information listed above is required for the organization to self-certify with the Safe Harbor. Enforcement is predicated on the representations made by the organization through self-certification that it will follow the Safe Harbor in handling personal information transferred from Europe.

Optional Information: In addition, we ask for other information that will be of assistance to U.S. and European organizations:

1. *EU countries in which the organizations are currently doing business.* This will be used by EU organizations looking for Safe Harbor organizations for a specific task to be able to locate one easily using this list.

2. *Industry sector*. This will be used by EU organizations looking for Safe Harbor organizations for a specific task to be able to locate one easily using this list.

3. *Sales and number of employees.* This will allow the Department of Commerce to determine if we are reaching small and medium sized enterprises or if we need to do further outreach.

The collected information is not disseminated to the public.

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 Department of Commerce offers U.S. organizations the opportunity to provide the self-certification described above via the Department of Commerce's Safe Harbor website, located at http://export.gov/safeharbor . This electronic option allows the U.S. organization to be publicly recognized as being a Safe Harbor adherent and will further insure the accuracy of the U.S. organizations information available to the public. Organizations will indicate the name, title, phone number, and e-mail address of the individual certifying, and will click on a button to indicate that the individual has the right to provide this attestation. Approximately 99.5% of all new applicants for certification use the electronic option. Since online renewal of existing certification was offered in April 2009, nearly 95 percent of all renewals submitted are received online via the program's website.

4. Describe efforts to identify duplication.

There is no duplication. The Safe Harbor is a unique method for handling personal data flows between the EU and the United States. Under the terms of our agreement with the European Commission, the U.S. Department of Commerce has the sole responsibility for collecting and making publicly available the list of organizations that self-certify to the Safe Harbor.

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

The Safe Harbor provides a number of important benefits to U.S. business, both small and large. Most importantly, it will provide predictability and continuity for U.S. organizations that receive personal information from Europe. All twenty seven (27) member countries are bound by the European Commission's finding of adequacy. The Safe Harbor also eliminates the need for prior approval to begin data transfers, or makes approval from the appropriate EU member countries automatic. The Safe Harbor offers a simpler, more efficient and less costly means of complying with the adequacy requirements of the EU Directive, which should particularly benefit small and medium sized enterprises.

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

Failure to establish a medium for U.S. organizations to self-certify would cause the U.S. Government to fail to implement the understanding reached between the European Commission and the United States. As a result, the flow of personally identifiable data between Europe and the United States could be seriously disrupted. Alternatives to Safe Harbor that exist under the European Union's legal framework for data protection are more burdensome, costly, and particularly injurious 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 October 12, 2010 (Volume 75, Number 196, pages 62502-62503). No comments from the public have been generated from this announcement.

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. The information provided by the respondents is public information and does not include any personally identifiable information. The respondents, who volunteer the information, know in advance that the information will be publicly available on the program's website consistent with Departmental 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 European Union related to receipt of personal data of EU 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	Total Hours
Website	20 minutes	575	575	191.67 hours
Letter	40 minutes	25	25	14.67 hours
		Total: 600	600	208.34 hours **(208)**

Cost to Respondents or record keepers: Total Hours (208.34) x Average Salary ($35.00/hour) = $7,291.90.

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).

Not Applicable.

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

Total estimated Cost to the Federal Government: **$10,500** - Based on 30 minutes to review and process each application (600) X average salary of $35 per hour.

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

The adjustment increase is based on a rise in the rate of self-certification (from 500 to 600 organizations estimated to sign-up/self-certify this year-CY 2011).

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

Some of the collected information is included in the List of Safe Harbor Participants which is on the 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.