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

Section A. Justification

1. Necessity of Information Collection

Introduction: 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 Department of Commerce consulted extensively with U.S. organizations affected by the European Directive and interested non-government organizations. On July 27, 2000, the European Commission issued its decision in accordance with Article 25.6 of the Directive that the Safe Harbor Privacy Principles provide 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 27, 2000, the Department of Commerce began working on the mechanisms that are necessary to put this accord into effect. The European Member States implemented the decision made by the Commission within 90 days. Therefore, 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 March 29, 2004, 474 U.S. organizations have placed themselves on the Safe Harbor List, located at http://export.gov/safeharbor.

Why is the information being collected?: 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. This 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.

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 15 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 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 the Safe Harbor's 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 and agrees to adhere to the Safe Harbor's requirements, which includes elements such as notice, choice, access, data integrity, security and enforcement.

2. Description and Practical Utility of the Information Collection Activity

The Department of Commerce maintains a list of all organizations that file self-certification letters and makes both the list and the self-certification letters publicly available. As of May 31, 2007, 1,171 organizations were on the Safe Harbor List. We anticipate that about 25-35 organizations a month will sign up. The total number of organizations on the Safe Harbor List should rise to about 1,350 in the next year. It is very difficult to determine exactly how many organizations will ultimately sign up. It is important to note though that organizations must annually reaffirm their adherence to the Safe Harbor.

This list will be most regularly used by European Union organizations to determine whether further information and contracts will be needed by a U.S. organization to receive personally identifiable information. It 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.

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 subject to the jurisdiction of one of these two enforcement bodies. This data 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 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. Enforcement is predicated on the representation s made by the organization through self-certification that it will follow the Safe Harbor in handling personal information transferred from Europe.

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.

3. Uses of Automated 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 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 certifying individual, and will click on a button to indicate that the individual has the right to provide this attestation.

4. Non-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 responsibility for collecting and making publicly available the list of organizations that self-certify to the Safe Harbor.

5. Minimizing the Burden for Small Business

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. Consideration of Alternatives

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.

7. Paperwork Reduction Act Guidelines

This information will be collected consistent with the Paperwork Reduction Act guidelines.

8. Consultations

The U.S. private sector was consulted extensively in the preparation of the Safe Harbor framework when the program was established in 1998 which included development of the documents supporting the framework and the collection of information required. There is an ongoing process throughout the years to obtain feedback from private sector organizations, trade associations, individuals, and consumer groups. We have also held private sector workshops and seminars on average of once every three months subject to the availability of resources. The most recent occurred twice during the month of March 2007 and once in February 2007. Additional individual consultations are held regularly with the legal and business communities.

A Federal Register notice soliciting public comment was published on April 17, 2007, Volume 72, Number 73, pages 19172-19173. No comments were received.

9. Incentives to Respondents

No payment or gifts are being offered to the respondents. Firms that self-certify are assured the benefits of the Safe Harbor.

10. Assurance of Confidentiality

Both the Safe Harbor framework and the self-certification guidelines in FAQ #6 state that the information provided will be made available to the public.

When self-certifying, U.S. organizations will also be asked to provide information about their number of employees and general information about their range of sales. As explained in item 2 above, this information is being collected only to determine if small businesses are taking advantage of the Safe Harbor. Providing this data is entirely voluntary and the Safe Harbor List will not disclose this information.

U.S. organizations will also be asked in which EU Member States they now do business. This information is voluntary but will allow European organizations to determine where U.S. organizations are currently doing business in their country and perhaps facilitate more business for the U.S. organizations.

11. Justification for Sensitive Information

No information of a sensitive nature is required.

12. Estimation of Government and Respondents' Burden Hours and Costs

We estimate that up to 500 organizations will choose to self-certify during this next year. The average time to complete and process the self-certifications is estimated at 20 minutes for website responses and 40 minutes for letter responses. We anticipate receiving 475 website and 25 letter responses. The estimated average private sector salary for persons responding is $35 per hour and average public sector salary for persons monitoring the input and updating the website is $35 per hour.

13. Costs to Respondents:

Type of Response	Time to Complete Self-Certifications	Number of Respondents	Number of Responses	Total Hours
Website	20 minutes	475	475	158.3 hours
Letter	40 minutes	25	25	16.7 hours
	Total:	500	500	175.0 hours

Cost to Respondents: Total Hours (175) x Average Salary ($35.00/hour) = $6,125.00

14. Costs to Federal Government:

Type of Response	Time to Process Self-Certifications	Number of Responses	Total Hours
Website	20 minutes	475	158.3 hours
Letter	40 minutes	25	16.7 hours
	Total:	500	175.0 hours

Cost to Government: Total Hours (175.0) x Average Salary ($35.00/hour) = $6,125.00

15. Rationale for Program Changes or Adjustments

No changes or adjustments.

16. Uses of Analytical Methodology

None.

17. Reasons for Not Displaying Expiration Data

None.

18. Rationale for Exceptions to Certification

None.

Section B. Collections of Information Employing Statistical Methods

This collection of information does not employ statistical methods.