SUPPORTING STATEMENT
EU-U.S. PRIVACY SHIELD FRAMEWORK SELF-CERTIFICATION FORM
OMB CONTROL NO. XXXX-XXXX

A. JUSTIFICATION

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

The purpose of this emergency request of Paperwork Reduction Act (PRA) clearance is to allow the Department of Commerce (DOC), as represented by the International Trade Administration (ITA), to collect information from organizations in the United States to enable such organizations' self-certification to the EU-U.S. Privacy Shield Framework (Privacy Shield). Given the critical role of the collection of information to the Privacy Shield, the importance to transatlantic commerce of providing the Privacy Shield without further delay, and the uncertainty regarding when the Privacy Shield would clear the final stage of the multi-stage European Union (EU) approval process, the DOC cannot reasonably comply at present with the normal clearance procedures.

The United States and the EU share the goal of enhancing privacy protection for their citizens, but take different approaches to protecting personal data. Given those differences, the DOC has developed the Privacy Shield in consultation with the European Commission, as well as with industry and other stakeholders, to provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the EU while ensuring the protection of the data as required by EU law.

The DOC had previously developed in consultation with European Commission the analogous U.S.-EU Safe Harbor Framework (Safe Harbor), which has been administered by the ITA since 2000 and had enabled transfers of personal data supporting billions of dollars in transatlantic trade. For over 15 years the Safe Harbor provided thousands of organizations in the United States and their partners on both sides of the Atlantic with a reliable mechanism for personal data transfers to the United States from the EU. In October 2015, the European Court of Justice (ECJ) invalidated the decision made by the European Commission in 2000, which had recognized the Safe Harbor as a valid legal mechanism for such transfers. The ECJ judgment has created considerable uncertainty with regard to transatlantic business arrangements and imposed associated costs, as the remaining legal data transfer mechanisms are not only time-consuming and costly to implement, but also potentially subject to similar legal challenges.

In February 2016, the United States and European Commission reached agreement on and published the Privacy Shield, including the Privacy Shield Principles, which reflect over two years of discussions about enhancing the provisions of the Safe Harbor. Following the February 2016 announcement, the European Commission submitted the Privacy Shield for review and approval by the EU.

Upon receiving EU approval on July 12, the DOC is issuing the Privacy Shield Principles under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The ITA will administer and supervise the Privacy Shield, including by maintaining and making publicly available an authoritative list of U.S. organizations that have self-certified to the DOC. In order to rely on the Privacy Shield for transfers of personal data from the EU, an organization must self-certify its adherence to the Privacy Shield Principles to the DOC, be

placed by the ITA on the Privacy Shield List, and remain on the Privacy Shield List.

ITA is publishing a separate federal register notice that explains the fee structure for Privacy Shield. ITA will review comments on that notice and respond to them at a later time.

To self-certify for the Privacy Shield, an organization must provide to the DOC a self-certification submission that contains the information specified in the Privacy Shield Principles. The Privacy Shield self-certification form, the proposed information collection, would be the means by which an organization would provide the relevant information to the ITA. The proposed Privacy Shield self-certification form is substantially similar to the information collection request approved by OMB in connection with the Safe Harbor self-certification form (OMB Control No. 0625-0239).

We request that the PRA review be completed within 180 days from receipt of this submission.

2. 1Explain how, by whom, how frequently, and for what purpose the information will be used. 1If 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.

In order to rely on the Privacy Shield, an organization must self-certify its adherence to the Privacy Shield Principles to the Department of Commerce (DOC). While the decision by an organization to enter the Privacy Shield is entirely voluntary, effective compliance is compulsory: an organization that self-certifies to the DOC and publicly declares its commitment to adhere to the Privacy Shield Principles must comply fully with the Principles.

To self-certify for the Privacy Shield, an organization must provide to the DOC a self-certification submission, signed by a corporate officer on behalf of the organization that is joining the Privacy Shield that contains at least the following information:

- name of organization, mailing address, e-mail address, telephone, and fax numbers;

- description of the activities of the organization with respect to personal information received from the EU, including: a list of all entities or subsidiaries of the organization that are also adhering to the Privacy Shield Principles and are covered under the organization's self-certification, types of personal data covered by the organization's self-certification, and the purposes for which the organization processes personal data in reliance on the Privacy Shield, and

- description of the organization's privacy policy for such personal information, including:
    - if the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public;
    - its effective date of implementation;
    - a contact office for the handling of complaints, access requests, and any other issues arising under the Privacy Shield;
    - the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of

laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
- name of any privacy program in which the organization is a member;
- method of verification *(e.g.,* in-house, third party); and
- the independent recourse mechanism that is available to investigate unresolved complaints.

The DOC will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the DOC and declared their commitment to adhere to the Privacy Shield Principles ("the Privacy Shield List"), as well as an authoritative record of U.S. organizations that had previously self-certified to the DOC, but that have been removed from the Privacy Shield List. The DOC will maintain the list of organizations that file completed self-certification submissions, thereby assuring the availability of Privacy Shield benefits, and will update such list on the basis of re-certification submissions, which must be provided not less than annually, and notifications received of non-compliance. The DOC will remove an organization from the Privacy Shield List if it fails to complete its annual re-certification to the DOC, voluntarily withdraws from the Privacy Shield, or has persistently failed to comply with the Privacy Shield Principles.

The Privacy Shield List will be used not only by individuals and organizations in the EU and organizations in the United States to confirm whether a given organization is entitled to the benefits of the Privacy Shield, but also by U.S. and European authorities in the context of alleged non-compliance with the Privacy Shield Principles.

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 will offer U.S. organizations the opportunity to provide the self-certification described above via the DOC's Privacy Shield website: www.privacyshield.gov. Organizations interested in participating in the Privacy Shield will make their initial self-certification, as well as annual re-certification submissions, including payment of the relevant processing fee, online via the Privacy Shield website. The Privacy Shield website also provides organizations already in the program with direct access to their record, thereby enabling them to update the information provided therein throughout the year. This electronic method will be employed, as it is expressly designed to process submissions in a timely and accurate manner. An organization cannot make an initial self-certification, as well as annual re-certification submissions, or other updates to an existing submission via the DOC's Privacy Shield website unless it has registered a username and password.

4. Describe efforts to identify duplication.

There is no duplication. The EU-U.S. Privacy Shield Framework is a unique method for handling personal data flows between the EU and the United States. Under the terms of the DOC's agreement with the European Commission, the DOC has the sole responsibility for collecting and making publicly available the list of organizations that self-certify their adherence

to the Privacy Shield Principles.

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

There will likely be small businesses amongst the organizations seeking to self-certify under the Privacy Shield. The burden associated with the information collection is not considered to be significant, because the estimated time to complete the self-certification form is 40 minutes. The burden is being minimized by keeping the information request as simple as possible and limiting areas of inquiry to those essential to fulfilling the request.

The EU-U.S. Privacy Shield Framework provides 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. All 28 EU Member States will be bound by the European Commission's finding of "adequacy". The Privacy Shield offers a simpler and more cost-effective means of complying with the relevant requirements of the EU Directive, 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.

Preventing or limiting the collection of information associated with self-certification under the Privacy Shield would prevent the U.S. Government from implementing the Privacy Shield Framework as agreed between the European Commission and the DOC. As a result, the flow of personal data from the EU and to the United States could be seriously disrupted, negatively impacting trade and investment. Alternatives to the EU-U.S. Privacy Shield Framework 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.

Collection of information will be made in a manner consistent with OMB guidelines.

8. Provide information on 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 OMB has waived the requirement that the DOC submit a PRA Federal Register Notice for the emergency approval of this information collection.

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

See above. The OMB has waived the requirement that the DOC submit a PRA Federal Register Notice for the emergency approval of this information collection.

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

With the exception of the information concerning level of sales and number of employees, which is provided optionally, the information provided by the respondents in their self-certification submissions will be made available to the public. The respondents, who volunteer the information, know in advance that, with the exception noted, the information will be made publicly available on the DOC's Privacy Shield 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.

No questions of a sensitive nature are included in this information collection.

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

The total expected number of Privacy Shield submissions that would be received within the first year of the program is 3600, with each submission representing a separate respondent. DOC estimates an average burden of 40 minutes per submission, including the time it would take to complete the self-certification form and submit it online via the Privacy Shield website. 3600 responses/submissions x 0.66 hours (i.e., 40 minutes) = 2376 hours total burden. Self-certification must be renewed annually using the same form.

Type of Response	Response Time	No. of Respondents	No. of Responses	Total Hours
Completion and submission of initial self-certification or recertification applications (electronically via DOC's Privacy Shield website)	0.66 hours (i.e., 40 minutes)	3,600	3,600	2,376

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).

The estimated annual cost burden to respondents, excluding the value of the burden hours in Question 12, is $2,824,200.

Note:

The DOC's ITA is implementing a cost recovery program to support the operation of the EU-U.S. Privacy Shield Framework, which will require that U.S. organizations pay an annual fee to the DOC in order to self-certify under the Privacy Shield. The cost recovery program will support the administration and supervision of the Privacy Shield program and support the provision of Privacy Shield-related services, including education and outreach. The fee a given organization will be charged will be determined according to a sliding scale based on the organization's annual revenue.

EU-U.S. Privacy Shield Framework Cost Recovery Program Fee Schedule:

Organization's Annual Revenue	
Under $5,000,000	$250
Over $5,000,000 - $25,000,000	$650
Over $25,000,000 - $500,000,000	$1,000
Over $500 million to $5 billion	$2,500
Over $5 billion	$3,250

As was noted in the answer to Question 12, 3,600 is the estimated number of Privacy Shield responses/submissions that would be received within the first year of the program.

Organization's Annual Revenue	Annual Fee	Estimated number of Privacy Shield submissions received the first year of the program	Cost Burden to Respondents
Under $5,000,000	$250	1,116 (i.e., 31% of 3,600)	$279,000
Over $5,000,000 - $25,000,000	$650	828 (i.e., 23% of 3,600)	$538,200
Over $25,000,000 - $500,000,000	$1,000	1,440 (i.e., 40% of 3,600)	$1,440,000
Over $500,000,000 to $5 billion	$2,500	180 (i.e., 5% of 3,600)	$450,000
Over $5 billion	$3,250	36 (i.e., 1% of 3,600)	$117,000
			Total = $2,824,200

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

Note: for purposes of calculating the monetary value of the burden in hours imposed per response on the Federal government, the Federal government employee's average salary is assumed to be $36.00/hour (i.e., the approximate, average hourly wage for the type of Federal government employee performing the relevant tasks)

Type of Response	Response Time	No. of Respondents	No. of Responses	Total Hours
Review and processing of initial self-certification or recertification applications (electronically via DOC's Privacy Shield website)	0.5 hours (i.e., 30 minutes)	3,600	3,600	1,800

Cost to Federal government per response: Response Time (30 minutes) x Average Salary ($36.00/hour) = $18.00

Total cost: Total Hours (1,800 hours) x Average Salary ($36.00/hour) = $64,800

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

This is a new information collection. This will replace the similar information collection for the U.S.-EU Safe Harbor program.

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 Privacy Shield List, which the DOC maintains (i.e., for the reasons discussed elsewhere in this supporting statement) on its Privacy Shield 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.

Not Applicable.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

This collection does not employ statistical methods.