

**SUPPORTING STATEMENT
U.S. DEPARTMENT OF COMMERCE
INTERNATIONAL TRADE ADMINISTRATION
INFORMATION COLLECTION FOR SELF-CERTIFICATION
TO THE EU-U.S. AND SWISS-U.S. PRIVACY SHIELD FRAMEWORKS
OMB CONTROL NO. 0625-0276**

A. JUSTIFICATION

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

The purpose of this 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. and/or Swiss-U.S. Privacy Shield Frameworks (Privacy Shield) and monitor organizations' compliance with the Privacy Shield Principles. The DOC previously requested and obtained approval of this information collection (OMB Control No. 0625-0276), which expires on 3/31/2020, and now requests approval of non-material changes to this information collection. These changes would clarify that the information collection instruments (i.e., the self-certification form, as well as questionnaires) may be used to collect information under both the EU-U.S. and the Swiss-U.S. Privacy Shield frameworks.

The United States and the European Union (EU) share the goal of enhancing privacy protection for their citizens, but take different approaches to protecting personal data. Given those differences, the DOC developed the EU-U.S. Privacy Shield Framework 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 United States developed the analogous Swiss-U.S. Privacy Shield Framework to provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from Switzerland while ensuring the protection of the data as required by Swiss law.

On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law, and the DOC began accepting EU-U.S. Privacy Shield self-certification submissions from organizations on August 1, 2016. On January 12, 2017, the Swiss Government deemed the Swiss-U.S. Privacy Shield Framework adequate to enable data transfers under Swiss law, and the DOC will begin accepting Swiss-U.S. Privacy Shield self-certification submissions from organizations on April 12, 2017.

The DOC has issued the Privacy Shield Principles under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The ITA administers and supervises 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 and/or Switzerland, an organization must submit information to ITA to self-certify its compliance with the Privacy Shield Principles. Participating organizations are required to respond to inquiries and requests by the ITA for information relating to Privacy Shield.

More information on the Privacy Shield is available at: <https://www.privacyshield.gov/welcome>.

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.

In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC), the Department of Transportation, or another statutory body that will effectively ensure compliance with the Privacy Shield Principles; (b) publicly declare its commitment to comply with the Privacy Shield Principles; (c) publicly disclose its privacy policies in line with the Privacy Shield Principles; and (d) fully implement them.

Self-certification to the DOC is voluntary; however, an organization's failure to comply with the Principles after its self-certification is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.

In order to rely on the Privacy Shield for transfers of personal data from the EU and/or Switzerland, 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.

To self-certify for the Privacy Shield, an organization must provide to the DOC a self-certification submission, which contains the information specified in the Privacy Shield Principles and is signed by a corporate officer on behalf of the organization that is seeking to join the Privacy Shield. The self-certification submission must contain 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 and/or Switzerland, 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;

- o 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);
- o name of any privacy program in which the organization is a member;
- o method of verification (*e.g.*, in-house, third party); and
- o 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, 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 Switzerland 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.

The DOC has committed to follow up with organizations that have been removed from the Privacy Shield List. The DOC will send questionnaires to organizations that fail to complete the annual certification or that have withdrawn from the Privacy Shield to verify whether the organization will return, delete, or continue to apply the Principles to the personal information that they received while they participated in the Privacy Shield, and if personal information will be retained, verify who within the organization will serve as an ongoing point of contact for Privacy Shield-related questions.

In addition, the DOC has committed to conduct compliance reviews on an ongoing basis, including by sending detailed questionnaires to participating organizations. In particular, such compliance reviews shall take place when: (a) the DOC has received specific non-frivolous complaints about an organization's compliance with the Principles, (b) an organization does not respond satisfactorily to inquiries by the DOC for information relating to the Privacy Shield, or (c) there is credible evidence that an organization does not comply with its commitments under the Privacy Shield.

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 Privacy Shield website: <https://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, 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.

It is anticipated that the Privacy Shield questionnaires and the corresponding responses provided by organizations would be conveyed electronically via e-mail or through the DOC Privacy Shield website.

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, and the Swiss-U.S. Privacy Shield Framework is a unique method for handling personal data flows between Switzerland and the United States. Under the terms of the DOC's agreements with the European Commission and the Swiss Government, 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 are 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 estimated completion time for three of the questionnaires is under 40 minutes per questionnaire, and the estimated completion time for the remaining questionnaire is 75 minutes. The burden is being minimized by keeping the information request as simple as possible and limiting areas of inquiry to those essential to meeting the requirements set forth in the Privacy Shield frameworks.

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 are bound by the European Commission's finding of "adequacy". The EU-U.S. Privacy Shield Framework offers a simpler and more cost-effective means of complying with the relevant requirements of the EU Directive, which particularly benefits small and medium enterprises. The Swiss-U.S. Privacy Shield Framework offers a simple and cost-effective means of complying with the relevant requirements of Swiss law, which similarly benefits 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.

Preventing or limiting the collection of information associated with self-certification and the questionnaires under the Privacy Shield would prevent the U.S. Government from implementing the EU-U.S. Privacy Shield Framework as agreed between the European Commission and the DOC, and the Swiss-U.S. Privacy Shield Framework as agreed between the Swiss Government and the DOC. As a result, the flow of personal data from the EU and Switzerland to the United States could be 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 waived the requirement that the DOC submit a PRA Federal Register Notice for the emergency approval of this information collection (OMB Control No. 0625-0276), which expired on 1/31/2017. Federal Register Notices requesting public comments concerning this information collection were published on November 9, 2016 (Volume 81, Number 2016-27053, pages 78775-78776), and January 23, 2017 (Volume 82, Number 2017-01334, pages 7796-7797). No comments from the public have been generated from these announcements. This information collection was subsequently approved resulting in the present expiration date of 3/31/2020.

A Federal Register Notice requesting public comments concerning the Swiss-U.S. Privacy Shield Framework information collection was published on January 19, 2017 (Volume 82, Number 2017-01156, pages 6492-6493). 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.

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. Through the DOC Privacy Shield website, the information submitted by organizations to the ITA to self-certify their compliance with Privacy Shield is made publicly available, with the exception of the information concerning annual revenue and number of employees. The exception is indicated in the self-certification form itself, as well as in guidance provided elsewhere on the website. The respondents who volunteer the information in their self-certification submissions 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 estimated annual burden in hours is 1,900.

The following refers to the estimates for the first year of the program in which both EU-U.S. and Swiss-U.S. Privacy Shield submissions are received.

Self-Certification Form

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. Self-certification must be renewed annually using the same form.

3,000 responses/submissions x 0.67 hours (i.e., 40 minutes) = 2,010 hours total burden.

| 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) | 0.67 hours (i.e., 40 minutes) | 3,000 per year | 3,000 per year | 2,010 per year |

Failure to Recertify Questionnaire

300 responses/submissions x 0.5 hours (i.e., 30 minutes) = 1150 hours total burden.

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|---|------------------------------|--------------------|------------------|---------------|
| Completion and submission of Failure to Recertify Questionnaire | 0.5 hours (i.e., 30 minutes) | 300 per year | 300 per year | 1150 per year |

Withdrawal Questionnaire

80 responses/submissions x 0.33 hours (i.e., 20 minutes) = 26.4 hours total burden.

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|---|-------------------------------|--------------------|------------------|---------------|
| Completion and submission of Voluntary Withdrawal Questionnaire | 0.33 hours (i.e., 20 minutes) | 80 per year | 80 per year | 26.4 per year |

Annual Questionnaire for Organizations that Indicated upon Withdrawal that They Would Retain Personal Data Received under the Privacy Shield

60 responses/submissions x 0.42 hours (i.e., 25 minutes) = 25.2 hours total burden.

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|---|-------------------------------|--------------------|------------------|---------------|
| Completion and submission of Annual Questionnaire for Organizations that Indicated upon Withdrawal that They Would Retain Personal Data Received under the Privacy Shield | 0.42 hours (i.e., 25 minutes) | 60 per year | 60 per year | 25.2 per year |

Compliance Review Questionnaire

200 responses/submissions x 1.25 hours (i.e., 75 minutes) = 250 hours total burden.

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|--|-------------------------------|--------------------|------------------|--------------|
| Completion and submission of Compliance Review Questionnaire | 1.25 hours (i.e., 75 minutes) | 200 per year | 200 per year | 250 per 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).

The estimated annual cost burden to respondents, excluding the value of the burden hours in Question 12, is \$2,953,875.

Note:

- The DOC’s ITA is implementing a cost recovery program to support the operation of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, 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 annual fee a given organization will be charged will be determined according to a sliding scale based on the organization’s annual revenue.

Privacy Shield Cost Recovery Program Fee Schedule:

| Organization’s Annual Revenue | Single Framework | Both Frameworks |
|-----------------------------------|------------------|-----------------|
| Under \$5,000,000 | \$250 | \$375 |
| Over \$5,000,000 - \$25,000,000 | \$650 | \$975 |
| Over \$25,000,000 - \$500,000,000 | \$1,000 | \$1,500 |
| Over \$500 million to \$5 billion | \$2,500 | \$3,750 |
| Over \$5 billion | \$3,250 | \$4,875 |

As was noted in the answer to Question 12, 3,000 is the estimated number of Privacy Shield responses/submissions that would be received within the first year of the program in which both EU-U.S. and Swiss-U.S. Privacy Shield submissions are received.

| Organization's Annual Revenue | Annual Fee | Estimated number of Privacy Shield submissions received per year covering both frameworks | Cost Burden to Respondents |
|-----------------------------------|------------|---|----------------------------|
| Under \$5,000,000 | \$375 | 465 (i.e., 31% of 1,500) | \$174,375 |
| Over \$5,000,000 - \$25,000,000 | \$975 | 345 (i.e., 23% of 1,500) | \$336,375 |
| Over \$25,000,000 - \$500,000,000 | \$1,500 | 600 (i.e., 40% of 1,500) | \$900,000 |
| Over \$500,000,000 to \$5 billion | \$3,750 | 75 (i.e., 5% of 1,500) | \$281,250 |
| Over \$5 billion | \$4,875 | 15 (i.e., 1% of 1,500) | \$73,125 |
| | | | Total = \$1,765,125 |

| Organization's Annual Revenue | Annual Fee | Estimated number of Privacy Shield submissions received per year covering a single framework | Cost Burden to Respondents |
|-----------------------------------|------------|--|----------------------------|
| Under \$5,000,000 | \$250 | 465 (i.e., 31% of 1,500) | \$116,250 |
| Over \$5,000,000 - \$25,000,000 | \$650 | 345 (i.e., 23% of 1,500) | \$224,250 |
| Over \$25,000,000 - \$500,000,000 | \$1,000 | 600 (i.e., 40% of 1,500) | \$600,000 |
| Over \$500,000,000 to \$5 billion | \$2,500 | 75 (i.e., 5% of 1,500) | \$187,500 |
| Over \$5 billion | \$3,250 | 15 (i.e., 1% of 1,500) | \$48,750 |
| | | | Total = \$1,176,750 |

- The follow-up questionnaires sent by the DOC to U.S. organizations regarding their compliance with the Privacy Shield do not themselves require payment of a fee to the DOC. Organizations that withdraw from Privacy Shield, which choose to retain personal information received in reliance upon the Privacy Shield by continuing to apply the Privacy Shield Principles to such data, must affirm to the DOC, on an annual basis, their commitment to apply the Principles to such data. It is anticipated that such organizations will be charged an annual fee to support the additional administrative burden associated with this option.

| | | |
|------------|---|----------------------------|
| Annual Fee | Estimated number of organizations that withdraw from Privacy Shield per year, which choose to retain personal information received in reliance upon the Privacy Shield by continuing to apply the Privacy Shield Principles to such data that must affirm to the DOC, on an annual basis, their commitment to apply the Principles to such data | Cost Burden to Respondents |
| \$200 | 60 | \$12,000 |

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

\$278,779.32 is the total estimated annualized cost to the Federal government according to the methodology described below; however, this figure does not reflect significant website development costs associated with the DOC’s Privacy Shield website. The DOC’s Privacy Shield website, which performs multiple functions essential to Privacy Shield, has required and continues to require significant investment in terms of time and resources.

Note: This estimate is calculated by first determining the hourly rate, and the estimated time that it takes to process the form or questionnaire. The hourly rate is calculated by taking the approximate GS rating/step for the type of employee performing the relevant tasks and adding 30% to that rate to account for overhead and other basic costs. For purposes of this calculation \$36.14/hour is assumed to be the approximate GS rating/step; therefore, the rate used is \$46.98 (\$36.14 + \$10.84).

Self-Certification Form

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|---|--------------------------------|--------------------|------------------|----------------|
| Review and processing of initial self-certification or recertification applications | 1.67 hours (i.e., 100 minutes) | 3,000 per year | 3,000 per year | 5,010 per year |

Cost to Federal government per response: Response Time (1.67 hours) x Hourly Rate (\$46.98/hour) = \$78.46

Total cost: Total Hours (5,010 hours) x Hourly Rate (\$46.98/hour) = \$235,369.80

Failure to Recertify Questionnaire

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|---|-------------------------------|--------------------|------------------|--------------|
| Review and processing of Failure to Recertify Questionnaire | 1.33 hours (i.e., 80 minutes) | 300 per year | 300 per year | 399 per year |

Cost to Federal government per response: Response Time (1.33 hours) x Hourly Rate (\$46.98/hour) = \$62.48

Total cost: Total Hours (399 hours) x Hourly Rate (\$46.98/hour) = \$18,745.02

Voluntary Withdrawal Questionnaire

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|---|---------------------------|--------------------|------------------|-------------|
| Review and processing of Voluntary Withdrawal Questionnaire | 1 hour (i.e., 60 minutes) | 80 per year | 80 per year | 80 per year |

Cost to Federal government per response: Response Time (1 hour) x Hourly Rate (\$46.98/hour) = \$46.98

Total cost: Total Hours (80 hours) x Hourly Rate (\$46.98/hour) = \$3,758.40

Annual Questionnaire for Organizations that Indicated upon Withdrawal that They Would Retain Personal Data Received under the Privacy Shield

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|--|-------------------------------|--------------------|------------------|-------------|
| Review and processing of Annual Questionnaire for Organizations that Indicated upon Withdrawal that They Would Retain Personal Data Received | 0.75 hours (i.e., 45 minutes) | 60 per year | 60 per year | 45 per year |

| | | | | |
|--------------------------|--|--|--|--|
| under the Privacy Shield | | | | |
|--------------------------|--|--|--|--|

Cost to Federal government per response: Response Time (0.75 hours) x Hourly Rate (\$46.98/hour) = \$35.24

Total cost: Total Hours (45 hours) x Hourly Rate (\$46.98/hour) = \$2,114.10

Compliance Review Questionnaire

| Type of Response | Response Time | No. of Respondents | No. of Responses | Total Hours |
|--|-----------------------------|--------------------|------------------|--------------|
| Review and processing of Compliance Review Questionnaire | 2 hours (i.e., 120 minutes) | 200 per year | 200 per year | 400 per year |

Cost to Federal government per response: Response Time (2 hours) x Hourly Rate (\$46.98/hour) = \$93.96

Total cost: Total Hours (400 hours) x Hourly Rate (\$46.98/hour) = \$18,792

(Self-Certification Form total: \$235,369.80) + (Failure to Recertify Questionnaire total: \$18,745.02) + (Voluntary Withdrawal Questionnaire total: \$3,758.40) + (Annual Questionnaire for Organizations that Indicated upon Withdrawal that They Would Retain Personal Data Received under the Privacy Shield total: \$2,114.10) + (Compliance Review Questionnaire total: \$18,792) = \$278,779.32

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

This information collection (OMB Control No. 0625-0276) replaces the similar information collection for the U.S.-EU and U.S.-Swiss Safe Harbor programs.

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 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.