

Supporting Statement for Paperwork Reduction Act Submissions

Title: OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM)

OMB Control Number: 1600-0006

OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM) Supporting Statement A

A. Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

Throughout the 1990s and culminating in the terrorist attacks of September 11, 2001, there was a growing concern, both in Congress and across the border management community, that the border officials lacked the necessary information and technology to manage the entry/exit process and enforce the relevant laws as effectively as possible. Congressional concerns included visa overstays, the number of foreign nationals in the country illegally, overall border security issues, and a need to expedite legitimate trade and travel. As a result, Congress passed a number of laws aimed at addressing many of these and other border-related issues, including requiring the border management community to develop a biometric based entry and exit system capable of improving the information resources available to immigration and border management decision-makers.

The Department of Homeland Security (DHS) established the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program in 2003 in order to meet specific legislative mandates intended to strengthen border security, address critical needs in terms of providing decision-makers with critical information, and demonstrate progress toward performance goals for national security, expediting of trade and travel, and supporting immigration system improvements. On March 26, 2013, the Consolidated and Further Continuing Appropriations Act, 2013 transitioned the core of US-VISIT's most significant and cross-cutting responsibilities to the newly created Office of Biometric Identity Management (OBIM).

By providing decision makers with the information they need where and when they need it, US-VISIT – now OBIM – is helping to make U.S. immigration and border management efforts more collaborative, more streamlined and more effective.

Copies of statutes and regulations associated with the collection were submitted with the prior initial submission, but briefly, the statutes that authorize DHS to collect biometric information from foreign nationals include but are not limited to: Sections 403(c) and 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, [Public Law 107-56, 115 Stat. 271](#), 344, 353 (Oct. 26, 2001); Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002,

[Public Law 107-173, 116 Stat. 543](#), 552 (May 14, 2002); Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004, [Public Law 108-458, 118 Stat. 3638](#), 3817 (Dec. 17, 2004); and Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, [Public Law 110-53, 121 Stat. 266, 338](#) (Aug. 3, 2007). DHS provided detailed abstracts of the particular sections of the then-existing statutes that established and authorized an entry-exit system that uses biometrics in prior rulemakings. *See, e.g.*, 69 Fed. Reg. 468 (Jan. 5, 2004); [69 Fed. Reg. 53318 \(Aug. 31, 2004\)](#); 73 Fed. Reg. 22065 (Apr. 24, 2008).

On July 27, 2006, DHS published a notice of proposed rulemaking proposing to expand the population of aliens subject to biometric requirements to include lawful permanent residents and other categories of immigrants. 71 Fed. Reg. 42605. DHS published the final rule, entitled “United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT); Enrollment of Additional Aliens in US-VISIT; Authority To Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry,” on December 19, 2008. *See* 73 Fed. Reg. 77473.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

DHS collects and disseminates information from individuals during their entry into and exit from the United States. This information is disseminated to specific DHS components; other Federal agencies; Federal, state, and local law enforcement agencies; and the Federal intelligence community to assist in the decisions they make related to, and in support of, the homeland security mission. Additionally, information may be shared with international partners in support of counter terrorism and international travel security. Information shared includes biographic, travel history, travel document, and biometric information (photographs and fingerscans) pertaining to covered individuals. No personally identifiable information is collected other than that which is necessary and relevant for the purposes of OBIM.

Individuals subject to the biometric requirements and processes (“covered individuals”) are nearly all persons who are not U.S. citizens at the time of entry or exit. *See* 8 C.F.R. § 235.1(f). Non-U.S. citizens who later become U.S. citizens will no longer be covered by the biometric requirement for entry and exit recording purposes, but the information about them collected by DHS while they were noncitizens will be retained, as will information collected about citizens who did not identify themselves as such. *See DHS/NPPD/USVISIT/PIA-001 US-VISIT, Increment 1, December 18, 2003.*

OBIM’s mission is to store, maintain, and share information, including biometric identifiers, on foreign nationals to assist U.S. Government officials in determining whether individuals (1) should be prohibited from entering the United States; (2) can receive, extend, change, or adjust immigration status; (3) have overstayed or otherwise violated the terms of their admission; (4) should be apprehended or detained for law enforcement action; or (5) need special protection/attention (e.g., refugees). OBIM provides biometric identification and analysis for homeland security decision makers. Additionally, OBIM supports DHS programs ability to:

- electronically verify – using biometrics – that the person presenting a credential is the person to whom it was issued;

- make biometrically-based screening information available for subsequent interactions by DHS programs and support recurrent vetting based on biometrics;
- store and match biometrics associated with DHS and other agency encounters with links to the appropriate case tracking systems and provide the ability for biometrics to be associated with multiple credentials; and
- ensure opportunities for redress and provide a mechanism for individual to ask for correction of their including biometric records.

Personal information that DHS collects will be used only for the purposes for which it was collected, unless other uses are specifically authorized or mandated by law. This collected information is principally accessed by Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), and Consular Officers of the Department of State (DOS). Appropriate Federal, state, local, or foreign government law enforcement agencies may use this information when needed to carry out their law enforcement responsibilities in support of the DHS immigration enforcement mission. Additionally, the Office of Personnel Management (OPM), the Transportation Security Agency (TSA), and other federal agencies use this information for background checks and granting access to critical transportation infrastructure.

All information collected is kept secure and confidential, and will not be discussed with, nor disclosed to, anyone within or outside DHS except in conjunction with their official duties as authorized by law. The DHS Chief Privacy Officer reviews pertinent aspects and conducts information audits to ensure that proper safeguards are in place and being adhered to appropriately, and that counsel and guidance concerning privacy information management and accessibility are provided.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

Numerous statutes provide for the creation of an integrated and automated system to record the arrival and departure of aliens; the deployment of equipment at all ports of entry to verify aliens' identities and authenticate travel documents through the comparison of biometric identifiers; and the recording of alien arrival and departure information from biometrically authenticated travel documents.¹

¹ See Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000, [Public Law 106-215, 114 Stat. 337](#) (June 15, 2000); Section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106-396, 114 Stat. 1637, 1641 (Oct. 30, 2000); Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, [Public Law 107-56, 115 Stat. 271](#), 353 (Oct. 26, 2001); Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002, [Public Law 107-173, 116 Stat. 543](#), 552 (May 14, 2002); Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004, [Public Law 108-458, 118 Stat. 3638](#), 3817 (Dec. 17, 2004); and Section 711 of the Implementing Recommenda-

OBIM information technology is designed to accurately collect the necessary information as quickly as possible. To achieve these goals of speed and accuracy, OBIM relies heavily on automated, electronic, and other technological collection techniques. OBIM has deployed equipment and software so that CBP Officers can biometrically compare and authenticate travel documents that the Departments of State and Homeland Security issue to aliens. Digital cameras are used to collect photos and digital fingerprint scanners collect fingerprint images from aliens seeking entry into the United States through our ports of entry. This has greatly improved CBP's ability to detect document fraud during the inspection process and has prevented over 8,000 known criminals and immigration law violators from entering the U.S. since these procedures were implemented on January 5, 2004.

The biometrics the aliens provide are entered into the OBIM Automated Biometric Identification System (IDENT). The alien's biometric and other information will be checked against law enforcement and intelligence data to determine whether the alien is a threat to national security or public safety, or is otherwise inadmissible.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

Immigration and border security management is provided by a number of entities within the Departments of Homeland Security, State, and Justice. The border management agencies created an Integrated Project Teams (IPT) to ensure that various agencies were not duplicating information collection from foreign nationals during the entry or exit processes. Consequently, the data collection executed by DHS is not duplicative of other DHS efforts.

OBIM's functionality is currently supported by more than 16 different information technology systems, including those managed by the Department of State, CBP, ICE, USCIS, the Federal Bureau of Investigation (FBI), the Department of Defense, and INTERPOL. The ability to exchange real-time, transaction-level data in a secure fashion represents an increasing need across the immigration and border management community. OBIM has prepared the foundation for the next challenging portion of the program, which calls for replacing existing "stove-piped" systems with integrated systems designed to support a reengineered border management process with the latest technology available.

5. If the collection of information impacts small businesses or other small entities (Item 5 of OMB Form 83-I), describe any methods used to minimize.

The collection of information does not have an impact on small businesses or other small entities.

6. Describe the consequence to Federal/DHS program or policy activities if the collection of information is not conducted, or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

tions of the 9/11 Commission Act of 2007, [Public Law 110-53, 121 Stat. 266, 338](#) (Aug. 3, 2007).

It is crucial to border security decision makers and law enforcement officials that they have access to timely and accurate information on the biometric-based identification of individuals DHS works with the Department of Justice (DOJ), DOS, and the Intelligence Community to collect and share this critical information. Reduction of the information collection requirements for DHS cannot occur without depriving immigration and border security decision makers of critical and timely admissibility and national security information, and would be in direct contravention of numerous existing statutory requirements, including Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 and Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:

- (a) Requiring respondents to report information to the agency more often than quarterly.
- (b) Requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it.
- (c) Requiring respondents to submit more than an original and two copies of any document.
- (d) Requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years.
- (e) In connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study.
- (f) Requiring the use of a statistical data classification that has not been reviewed and approved by OMB.
- (g) That includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use.
- (h) Requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

- (a) Respondents submit information (biometric fingerscans and visa/passport information) based upon the frequency of their travel into the United States. Moreover, the information collection is required by law each time aliens apply for immigration benefits or seek entry into (and eventually exit from) the United States. Frequent travel to and from the United States may cause respondents to submit information more often than quarterly. Information is updated as needed.
- (b) Not applicable. The collection of information from respondents is through electronic devices. No written responses are collected.
- (c) Not applicable. The collection of information from respondents is through electronic devices.
- (d) Not applicable. Respondents are not required to retain records in connection with this information collection.
- (e) Aside from mandated reports to Congress, there are no statistical aspects to this information collection.
- (f) Aside from mandated reports to Congress, there are no statistical aspects to this information collection.

- (g) Not applicable. No such requirement has been imposed.
- (h) Not applicable. No such requirement has been imposed.

8. Federal Register Notice:

- a. Provide a copy and identify the date and page number of publication in the Federal Register of the agency’s notice soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.
- b. Describe 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.
- c. Describe consultations with representatives of those from whom information is to be obtained or those who must compile records. Consultation should occur at least once every three years, even if the collection of information activities is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

| | Date of Publication | Volume Number | Number | Page Number | Comments Addressed |
|---------------------------------------|----------------------------|----------------------|---------------|--------------------|---------------------------|
| <i>60Day Federal Register Notice:</i> | 04/15/2013 | 78 | 72 | 22274 | Three comments received |
| <i>30-Day Federal Register Notice</i> | 07/23/2013 | 78 | 141 | 44136 | |

A 60-day Federal Register notice (FRN) (see attached) was published on April 15, 2013, requesting public comments. DHS received three comments in response to that notice. Two of the comments did not address the biometric data collection discussed in the FRN and thus are not addressed in this notice. The lone other comment came from a public interest research group that raised several privacy concerns, each of which is discussed below.

The commenter stated that DHS should impose strict information security safeguards and limit the dissemination of biometric information. Biometric information disseminated from IDENT, the target architecture for the collection and use of biometrics by DHS programs, is provided to Federal, state, local, foreign, or international government agencies that have entered into agreements with DHS, through OBIM, for biometric identification and analysis services. These agreements define the terms of security and dissemination needed to appropriately share information. DHS may share IDENT data (with the consent of the collection’s data owner and in accordance with the Routine Uses published in the applicable Privacy Act System of Records Notice, and other policies, and regulations) for the purposes of national security, law enforcement, immigration, intelligence, and other mission-related functions as determined by DHS. Through the practice of Fair Information Practice Principles (FIPPs) and other information safeguarding policies and procedures, each data owner is able to restrict the maintenance, retention, and sharing of its data with other organizations. For example,

organization-level data filtering is applied to asylum data so that only approved organizations can access that data.

The commenter recommended that DHS conduct a comprehensive Privacy Impact Assessment (PIA) of OBIM. DHS recognizes the importance of privacy and has published several PIAs to inform the public of how biometric data is being collected, the purpose of collection, the principal users of the data, and how the data will be used, shared, accessed, and stored. DHS published a new consolidated IDENT PIA on December 7, 2012. The new PIA retired the IDENT PIAs of July 31, 2006, and May 25, 2007; the US-VISIT/DHS and United Kingdom Border Agency's (UKBA) International Group Visa Services Project PIA of July 2, 2008; and the Five Country Conference (FCC) PIA of November 2, 2009. The consolidation of the aforementioned PIAs, and inclusion of initiatives including sharing with the Department of Defense and the Preventing and Combating Serious Crime initiative, provides the public with a more comprehensive view of IDENT activities and increases transparency into how the system uses personally identifiable information (PII) and details the system's sharing partners and functions. DHS continues to update its PIAs to ensure the transparency of its biometric and information sharing activities. PIAs can be found on the DHS Website at <http://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd>.

The commenter also recommended that DHS grant all individuals in IDENT the privacy rights afforded under the Privacy Act of 1974 (Privacy Act), 5 U.S.C. § 552a, as amended, which provides statutory privacy rights to U.S. Persons (U.S. citizens and Lawful Permanent Residents). DHS already does so. Although the Privacy Act does not cover visitors or aliens, as a matter of DHS policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a "mixed system" by DHS – a system that contains information on both U.S. Persons and non-U.S. Persons – shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Lawful Permanent Resident, visitor, or alien.

Additionally, the commenter objected to Privacy Act exemptions declared for the Arrival and Departure Information System (ADIS), which is not a biometric collection system. Pursuant to exemptions 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of IDENT are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), IDENT is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), and (e)(4)(H). Exemptions from these particular subsections are justified, on a case-by-case basis, to be determined at the time a request is made. The exemptions are standard law enforcement and national security exemptions exercised by a large number of Federal law enforcement and intelligence agencies. In appropriate circumstances, where compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived. The reasoning behind these exemptions is further detailed in IDENT Final Rule for Privacy Act Exemptions 72 Fed. Reg. 38749 (July 16, 2007).

The commenter further recommended applying international privacy standards to the collection and use of personal information obtained from non-U.S. citizens. The Fair Information Practice

Principles (FIPPs) serve as the foundational principles for privacy policy and implementation at DHS. The FIPPs are a set of eight principles (Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing) that are a widely accepted framework that is at the core of the Privacy Act of 1974 and is mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The 1980 Organization of Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are built upon the same principles as FIPPs. Further, in 1995, a variation of these principles became the basis of the European Union Data Protection Directive. The FIPPs have been agreed upon by member countries, including the United States, through a consensus and formal ratification process and form the basis of many modern international privacy agreements and national laws.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

Not applicable. DHS does not provide payment or gifts to respondents in exchange for information provided to OBIM.

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

The Privacy Act of 1974 mandates that personal information solicited from the individual completing federal records and forms shall be kept confidential. The respondent is informed that the response is mandatory and that only authorized agency officials will have access to the information being provided. As noted above, while not required by the Privacy Act, DHS policy extends certain provisions of the Privacy Act to all alien's data stored in IDENT.

OBIM has published PIAs, which provide further, detailed guidance on how the Office ensures that personal information is used appropriately, protected from misuse and improper disclosure, and destroyed when no longer needed. Personal data is securely stored and made available only to authorized officials and selected law enforcement agencies on a need-to-know basis to help protect the nation against those who intend harm to U.S. citizens or visitors and to ensure integrity in our immigration system. We have attached recent PIAs for your review.

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. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent.

Not applicable. There are no questions of a sensitive nature.

12. Provide estimates of the hour burden of the collection of information. The statement should:

- a. Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. Unless directed to do so, agencies should not conduct special surveys to obtain information on which to base hour burden estimates. Consultation with a sample (fewer than 10) of potential respondents is desired. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance. Generally, estimates should not include burden hours for customary and usual business practices.
- b. If this request for approval covers more than one form, provide separate hour burden estimates for each form and aggregate the hour burdens in Item 13 of OMB Form 83-I.
- c. Provide estimates of annualized cost to respondents for the hour burdens for collections of information, identifying and using appropriate wage rate categories. The cost of contracting out or paying outside parties for information collection activities should not be included here. Instead, this cost should be included in Item 14.

(a) See below for incremental implementation of OBIM.

Annual Reporting Burden:

| | |
|--|--------------|
| a. Number of Respondents | 156,732,422 |
| b. Number of Responses per each Respondent | 1 |
| c. Total annual Reponses | 156,732,422 |
| d. Hours for Response | .0097 |
| e. Total Annual Reporting Burden | 1,520,300 |
| f. Total Public Cost | \$49,714,000 |

Total annual reporting burden hours are 1,520,300. This estimate is calculated by multiplying the number of respondents (156,732,422) by the frequency of response (1), by the hours per response (35 seconds or .0097 hours).

The estimate of 35 seconds for 10-print processing is based on a survey of about 20,000 samples taken from 35 air, land, and sea ports of entry. The current time estimate accounts for officer instructions, print capture, and photo capture. This information is calculated based on Fiscal Year 2012 statistics.

(b) There are no forms associated with this collection.

(c) Annual Public Cost

Total public cost is \$49,714,000. This estimate is based on the number of respondents multiplied by 35 seconds (.0097 hours) per response, multiplied by \$32.70 (average hourly rate) plus the number of responses (1).

Table A.12: Estimated Annualized Burden Hours and Costs

| Type of | Form | Number of | Number of | Average | Total | Average | Total |
|---------|------|-----------|-----------|---------|-------|---------|-------|
|---------|------|-----------|-----------|---------|-------|---------|-------|

| Respondent | Name | Respondents | Responses per Respondent | Burden per Response (in hours) | Annual Burden (in hours) | Hourly Wage Rate | Annual Respondent Cost |
|-------------------------|---------------------|-------------|--------------------------|--------------------------------|--------------------------|------------------|------------------------|
| International Travelers | In-Person Interview | 156,732,422 | 1 | 0.0097 | 1,520,300 | 32.70 | 49,714,000 |
| Total | In-Person Interview | 156,732,422 | 1 | 0.0097 | 1,520,300 | 32.70 | 49,714,000 |

13. Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14.)

The cost estimate should be split into two components: (1) a total capital and start-up cost component (annualized over its expected useful life); and (b) a total operation and maintenance and purchase of services component. The estimates should take into account costs associated with generating, maintaining, and disclosing or providing the information. Include descriptions of methods used to estimate major cost factors including system and technology acquisition, expected useful life of capital equipment, the discount rate(s), and the time period over which costs will be incurred. Capital and start-up costs include, among other items, preparations for collecting information such as purchasing computers and software; monitoring, sampling, drilling and testing equipment; and record storage facilities.

If cost estimates are expected to vary widely, agencies should present ranges of cost burdens and explain the reasons for the variance. The cost of purchasing or contracting out information collection services should be a part of this cost burden estimate. In developing cost burden estimates, agencies may consult with a sample of respondents (fewer than 10), utilize the 60-day pre-OMB submission public comment process and use existing economic or regulatory impact analysis associated with the rulemaking containing the information collection as appropriate.

Generally, estimates should not include purchases of equipment or services, or portions thereof, made: (1) prior to October 1, 1995, (2) to achieve regulatory compliance with requirements not associated with the information collection, (3) for reasons other than to provide information to keep records for the government, or (4) as part of customary and usual business or private practices.

There are no capital or start-up costs associated with this information collection. Any cost burdens to respondents as a result of this collection are identified in items 12 and 14.

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing and support staff), and any other expense that would have been incurred without this collection of information. You may also aggregate cost estimates for Items 12, 13, and 14 in a single table.

Cost Analysis:

| | |
|--------------------------------|--------------|
| Printing Cost | \$ 0.00 |
| Collecting and Processing Cost | \$63,853,000 |
| Total Cost to Program | \$63,853,000 |
| Fee Charge | \$ 0.00 |
| Total Cost to Government | \$63,853,000 |

Government Cost

The estimated cost of the program to the Government is \$63,853,000. This figure is calculated by using the estimated number of respondents (156,732,422) multiplied by 35 seconds (.0097), the time it takes the agency to collect and process the information, multiplied by \$42 (the fully loaded 2010 hourly rate for a CBP inspection officer at the GS-9 step 5 level with benefits).

| Cost Category | Form Name | Hours for Design/ Administration | Hours per Report | Number of Reports | Total Annual Burden (in hours) | Average Hourly Wage Rate | Total Annual Cost |
|---|-----------|----------------------------------|------------------|-------------------|--------------------------------|--------------------------|-------------------|
| *Table not applicable for this collection | | | | | | | |
| Total | | | | | | | |

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB Form 83-I. Changes in hour burden, i.e., program changes or adjustments made to annual reporting and recordkeeping **hour** and **cost** burden. A program change is the result of deliberate Federal government action. All new collections and any subsequent revisions of existing collections (e.g., the addition or deletion of questions) are recorded as program changes. An adjustment is a change that is not the result of a deliberate Federal government action. These changes that result from new estimates or actions not controllable by the Federal government are recorded as adjustments.

There has been no change to the information being collected, and no change in the burden to the public.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time

schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

DHS does not intend to employ the use of statistics or the publication thereof for this collection of information except in the mandated reports to Congress, as in reporting of overstates.

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

No specific form is utilized in the information collection process.

18. Explain each exception to the certification statement identified in Item 19 "Certification for Paperwork Reduction Act Submissions," of OMB Form 83-I.

DHS does not request an exception to the certification of this information collection.