DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0106]

Privacy Act of 1974; U.S. Immigration and Customs Enforcement–012 Visa Security Program (VSP) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new system of records titled, U.S. Immigration and Customs Enforcement DHS/ICE–012 Visa Security Program Records (VSPR). The purpose of the VSPR system is to manage, review, track, investigate, and document visa security reviews conducted by ICE agents pertaining to U.S. visa applicants and to document ICE visa recommendations to the U.S. State Department. VSPR contains information about individuals who have applied for U.S. visas and undergo a visa security review. VSPR also contains data maintained in the Office of International Affairs' Visa Security Program Tracking System (VSPTS–Net), a software application used by ICE to record, track, manage, and report visa security review activities. VSPTS–Net manages the workflow associated with visa security reviews by recording and tracking all visa applicant reviews, records checks, and follow-up investigative activities. Additionally, a Privacy Impact Assessment (PIA) for VSPTS–Net will be posted on the Department's privacy Web site (*see http://www.dhs.gov/privacy* and follow the link to ''Privacy Impact Assessments.'') Due to urgent homeland security and law enforcement mission needs, VSPTS–Net is currently in operation. Recognizing that ICE is publishing a notice of system of records for an existing system, ICE will carefully consider public comments, apply appropriate revisions, and republish the VSPR notice of system of records within 180 days of receipt of comments. A proposed rulemaking is also published in this issue of the **Federal Register** in which the Department proposes to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil and administrative enforcement requirements.

DATES: The established system of records will be effective October 30, 2009. Written comments must be submitted on or before October 30, 2009.

ADDRESSES: You may submit comments, identified by DHS–2009–0106, by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.
- *Docket:* For access to the docket to read background documents or comments received go to *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: Lyn Rahilly, (202–732–3300) Privacy Officer, U.S. Immigration and Customs Enforcement, 500 12th Street, SW., Washington, DC 20536; or Mary Ellen Callahan, (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Visa Security Program Records (VSPR) system of records is owned and maintained by the ICE Office of International Affairs (OIA). It consists of paper and electronic records created in support of the Visa Security Program, the purpose of which is to identify persons who may be ineligible for a U.S. visa because of criminal history, terrorism association, or other factors and convey that information to the State Department, which decides whether to issue the visa. VSPR contains records on visa applicants for whom a visa security review is conducted. The Visa Security Program Tracking System (VSPTS-Net) is a new OIA application scheduled to deploy in September 2009 that supports the management of ICE's Visa Security Program. ICE Special Agents use VSPTS-Net to record, track, and manage all visa security reviews performed by ICE. The VSPR system of records describes records maintained in VSPTS-Net and associated paper records.

In support of Section 428 of the Homeland Security Act of 2002, ICE deploys agents to U.S. embassies and consulates (''consular posts'') in high-risk areas worldwide to conduct security reviews of visa applications. ICE agents assigned to the Visa Security Program examine visa applications, initiate investigations of applicants who may be ineligible for a visa, coordinate with other law enforcement entities, and provide advice and training to the State Department. Through its Visa Security Program, ICE also participates in the Security Advisory Opinion (SAO) process. which is a U.S. Government mechanism to coordinate third-agency checks on visa applicants about whom the State Department has security-related concerns. Upon request from the State Department, ICE provides information from DHS record systems about visa applicants who are selected to undergo the SAO process. The State Department in turn provides the results of SAO checks to consular officers to aid in adjudicating visa applications. Like the ICE Special Agents located at consular posts abroad, ICE agents and analysts supporting SAO operations identify persons who may be ineligible for a U.S. visa because of criminal history, terrorism association, or other factors and convey that information to the State Department, which decides whether to issue the visa.

VSPTS-Net will be used to support the Visa Security Program activities described above by recording, tracking, and managing the SAOs and visa security reviews and documenting the results that are communicated to the State Department. VSPTS-Net will provide ICE agents with an intranet-based application that manages the workflow associated with visa security reviews and provides the necessary analytical, reporting and data storage capabilities. VSPTS-Net will also allow users (ICE employees and contractors) to record relevant visa application data, derogatory information about applicants, visa recommendation data. It also supports the generation of performance metrics for the Visa Security program as a whole. Ultimately, the system helps the Visa Security Program and the State Department prevent known and suspected terrorists, criminals, and other ineligible persons from obtaining U.S. visas. A PIA was conducted on VSPTS-Net because it is a new system that will maintain personally identifiable information (PII). The VSPTS-Net PIA is available on the Department of Homeland Security (DHS) Privacy Office Web site at *http://www.dhs.gov/privacy*.

The DHS/ICE–012 VSPR system of records will collect, use, disseminate, and maintain PII on persons who apply for a visa and undergo a visa security review. This collection of information is necessary for ICE to conduct visa

security reviews and to provide the State Department with a visa recommendation and/or information that is relevant to the applicant's eligibility for a visa under Federal law.

Consistent with DHS's information sharing mission, information stored in the VSPR system of records may be shared with other DHS components, as well as appropriate Federal, State, local, Tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

A proposed rulemaking is published in this issue of the **Federal Register** in which the Department proposes to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil and administrative enforcement requirements. Individuals may request information about records pertaining to them stored in DHS/ICE–012 VSPR system of records as outlined in the ''Notification Procedure'' section below. ICE reserves the right to exempt various records from release pursuant to exemptions 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2) of the Privacy Act.

This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/ICE–012 Visa Security Program Records (VSPR) system of records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this new system of records to the Office of Management and Budget and to Congress.

SYSTEM OF RECORDS:

DHS/ICE–012

SYSTEM NAME:

Visa Security Program Records (VSPR).

CLASSIFICATION:

Classified; Controlled Unclassified Information.

SYSTEM LOCATION:

Records are maintained at the U.S. Immigration and Customs Enforcement (ICE) Headquarters in Washington, DC, ICE field offices, and foreign embassies and consulates.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include:

(1) Individuals who apply for U.S. visas, and

(2) Other individuals who are identified on the visa application, such as the applicant's spouse, individuals traveling with applicant, application preparer's name, and individuals identified by the applicant as the person in the U.S. with whom the applicant will stay (hereafter, applicant point of contact).

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system may include:

(1) Biographic, employment, contact, and other types of information provided on the visa application, or by the applicant and others during interviews, such as name, address, phone number, e-mail address, date of birth, country of birth, nationality, passport number, information related to applicant's intended travel to the United States, spouse's name, names and relationships of individuals traveling with applicant, the application preparer's name, and the name and address of the applicant point of contact.

(2) Information obtained during a visa security review from interviews, public records, foreign governments, and U.S. government databases, such as the State Department's visa control number, lookout records, criminal history, admission, visa and immigration history, and records indicating a possible threat to homeland or national security due to terrorism or other reasons.

(3) Recommendations and/or other information provided by ICE to the State Department pertaining to visa applicants, and the State Department's decision on the visa application.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

8 U.S.C. 1103; 8 U.S.C. 1153–55; 8 U.S.C. 1201–1204; Section 428 of the Homeland Security Act of 2002; 22 CFR 41.122; Memorandum of Understanding between DHS, Federal Bureau of Investigation, and State Department Bureau of Consular Affairs on Improved Information Sharing Services signed July 18, 2009; Memorandum of Understanding Between the Secretaries of State and Homeland Security Concerning the Implementation of Section 428 of the Homeland Security Act of 2002 signed on September 26, 2003; Memorandum of Understanding between the Department of State, Bureau of Consular Affairs and the Department of Homeland Security, U.S. Immigration and Customs Enforcement for Cooperation in Datasharing signed on October 6, 2006; and Memorandum of Agreement Between the Department of State and the Department of Homeland Security Regarding the Sharing of Visa and Passport Records and Immigration and Naturalization and Citizenship Records signed on November 18, 2008.

PURPOSE(S):

(a) To manage, review, track, investigate, document, and report on visa security reviews conducted by ICE agents pertaining to U.S. visa applicants and to document ICE recommendations to the State Department on visa issuance;

(b) To facilitate communication among ICE personnel on matters pertaining to visa applications, visa holders, and visa security reviews;

(c) To enforce the provisions of the Immigration and Nationality Act, as amended; and

(d) To identify potential criminal activity, immigration violations, and threats to homeland security; to uphold

and enforce the law; and to ensure public safety.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when:

1. DHS or any component thereof;

2. Any employee of DHS in his/her official capacity;

3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to an individual that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, Tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena.

I. To Federal and foreign government intelligence or counterterrorism agencies when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

J. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.

K. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

L. To appropriate Federal, State, local, Tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

M. To appropriate Federal, State, local, Tribal, or foreign governmental agencies or multilateral governmental organizations where DHS is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance national security or identify other violations of law.

N. To third parties during the course of a visa security review to the extent necessary to obtain information pertinent to the review, provided disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

O. To international and foreign governmental authorities in accordance with law and formal or informal international arrangements.

P. To a Federal, State, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

Q. To a Federal, State, Tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) To assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

R. To the Federal Bureau of Investigation, the National Counter-Terrorism Center (NCTC), the Terrorist Screening Center (TSC), or other appropriate Federal agencies, for the integration and use of such information to protect against terrorism, if that record is about one or more individuals

known, or suspected, to be or to have been involved in activities constituting, in preparation for, in aid of, or related to terrorism. Such information may be further disseminated by recipient agencies to Federal, State, local, territorial, Tribal, and foreign government authorities, and to support private sector processes as contemplated in Homeland Security Presidential Directive/HSPD–6 and other relevant laws and directives, for terrorist screening, threat-protection and other homeland security purposes.

S. To appropriate Federal, State, local, Tribal, or foreign governmental agencies or multilateral government organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health risk, as practicable.

T. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The electronic records are stored on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved by visa applicant name, passport number, or visa control number.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The system maintains a real-time auditing function of individuals who access the system.

RETENTION AND DISPOSAL:

ICE is in the process of drafting a proposed record retention schedule for the information maintained in VSPR, including system information maintained in VSPTS–Net. ICE anticipates retaining the following records for 25 years after the date of review: visa security reviews where ICE has no adverse finding and does not object to the issuance of a visa, visa security reviews where ICE does not object to the issuance of a visa but provides derogatory information to the Department of State regarding the applicant, and visa security reviews where ICE recommends against the issuance of a visa, with no nexus to terrorism. ICE anticipates retaining the following records for 75 years after the date of review: visa security reviews where ICE recommends against the issuance of a visa due to a nexus to terrorism, or where ICE does not object to the issuance of the visa but provides terrorism-related information to the State Department regarding the applicant. ICE also anticipates that extracts of visa applicant data created for the purpose of creating VSPTS–Net records will be retained by ICE for one week and then destroyed/deleted.

SYSTEM MANAGER AND ADDRESS:

Visa Security Program Unit Chief, Office of International Affairs, U.S. Immigration and Customs Enforcement, 800 N. Capitol Street NW., Suite 300, Washington, DC 20536.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, ICE will consider requests individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0550, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov* or 1–866–431–0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Information is obtained from the visa application, the visa applicant, Federal databases, foreign governments, Interpol, Europol, employers, family members, public records, the Internet, and other individuals or entities from which information is collected during a visa security review.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), and (e)(4)(H), (e)(5) and (e)(8); (f); and (g). Pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), this system 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), (e)(4)(H), and (f). In addition, to the extent a record contains information from other exempt systems of records, DHS will rely on the exemptions claimed for those systems.

Dated: September 23, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–23522 Filed 9–29–09; 8:45 am]

BILLING CODE 9111–28–P

DEPARTMENT OF HOMELAND SECURITY

Federal Emergency Management Agency

[Docket ID: FEMA–2009–0001]

Agency Information Collection Activities: Proposed Collection; Comment Request

AGENCY: Federal Emergency Management Agency, DHS.

ACTION: Notice; 60-day notice and request for comments; new information collection; OMB No. 1660–NEW; FEMA Form 089–8, IBSGP Investment Justification Template.

SUMMARY: The Federal Emergency Management Agency, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on a proposed new information collection. In accordance with the Paperwork Reduction Act of 1995, this Notice seeks comments concerning the Intercity Bus Security Grant Program (IBSGP).

DATES: Comments must be submitted on or before November 30, 2009.

ADDRESSES: To avoid duplicate submissions to the docket, please use only one of the following means to submit comments:

(1) *Online.* Submit comments at *http://www.regulations.gov* under docket ID FEMA–2009–0001. Follow the instructions for submitting comments.

(2) *Mail.* Submit written comments to Office of Chief Counsel, Regulation and Policy Team, DHS/FEMA, 500 C Street, SW., Room 835, Wash, DC 20472–3100.

(3) *Facsimile.* Submit comments to (703) 483–2999.

(4) *E-mail.* Submit comments to *FEMA–POLICY@dhs.gov.* Include docket ID FEMA–2009–0001 in the subject line.

All submissions received must include the agency name and docket ID. Regardless of the method used for submitting comments or material, all submissions will be posted, without change, to the Federal eRulemaking Portal at *http://www.regulations.gov,* and will include any personal information you provide. Therefore, submitting this information makes it public. You may wish to read the Privacy Act notice that is available on the Privacy and Use Notice link on the Administration Navigation Bar of *www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Contact Alexander Mrazik, Program Analyst, Grant Programs Directorate, 202–786–9732 for additional information. You may contact the Records Management Branch for copies of the proposed collection of information at facsimile number (202) 646–3347 or e0mail address: *FEMA–Information-Collections@dhs.gov.*

SUPPLEMENTARY INFORMATION: The Intercity Bus Security Grant Program (IBSGP) is a DHS grant program that focuses on infrastructure protection activities. IBSGP is one tool among a comprehensive set of measures authorized by Congress and implemented by the Administration to help strengthen the nation's critical infrastructure against risks associated with potential terrorist attacks. Section 1532, Title XV of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (6 U.S.C. 1182), mandates the Secretary to establish a grant program for eligible private operators providing transportation by an over-the-road bus for security improvements and that the Secretary shall determine the requirements for grant recipients, including application requirements.

Collection of Information

Title: FEMA FY 2009 Preparedness Grants: Intercity Bus Security Grant Program (IBSGP).

Type of Information Collection: New information collection.

OMB Number: 1660–NEW.

Form Titles and Numbers: FEMA Form 089–8, IBSGP Investment Justification Template.

Abstract: The IBSGP Investment Justification Template is submitted with the application which provides narrative details on proposed investments. These Investment Justifications must demonstrate how proposed projects address gaps and deficiencies in current programs and capabilities and the ability to provide enhancements consistent with the purpose of the program and guidance provided by FEMA. The data from the IBSGP Investment Justification Template is collected to assist decision-making at all levels, although it is primarily used by individual application reviewers.

Affected Public: Business or other for-profit.

Estimated Total Annual Burden Hours: 280 hours.

TABLE A.12—ESTIMATED ANNUALIZED BURDEN HOURS AND COSTS

Type of respondent	Form name/form number	Number of respondents	Number of responses per respondent	Total number of responses	Avg. burden per response (in hours)	Total annual burden (in hours)	Avg. hourly wage rate*	Total annual respondent cost
Business or other for-profit.	IBSGP Investment Justification Template, FEMA Form 089–8.	56	1	56	5	280	$25.97	$7,271.60
Total		56				280		$7,271.60