may be retrieved by NOC tracker numbers, name, social security number and other identifiers listed under the Categories of Records Section. Most information is stored as free text and any word, phrase, or number is searchable.

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.

RETENTION AND DISPOSAL:

OPS is working with the DHS Records Officer to develop a NARA approved retention schedule.

SYSTEM MANAGER AND ADDRESS:

Director, Office of Operations Coordination and Planning, National Operations Center, Department of Homeland Security, Washington, DC 20528.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security is proposing to exempt this system from the notification, access, and amendment procedures of the Privacy Act. However, DHS/OPS will consider individual requests to determine whether or not information may be released. 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 OPS FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under "contacts."

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 Chief Privacy Officer and Chief Freedom of Information Act Officer, *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; and
- 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) may 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 contained in this system is obtained from subject individuals, other Federal, State, local and tribal agencies and organizations, domestic and foreign media, including periodicals, newspapers, and broadcast transcripts, public and classified data systems, reporting individuals, intelligence source documents, investigative reports, and correspondence.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3).

Dated: November 5, 2010.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–28566 Filed 11–12–10; 8:45 am]

BILLING CODE 9110–9A–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2010–0086]

Privacy Act of 1974; Department of Homeland Security National Protection and Programs Directorate—001 National Infrastructure Coordinating Center Records 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 is giving notice that it proposes to establish a new Department of Homeland Security system of records titled, "Department of Homeland Security National Protection and Programs Directorate—001 National Infrastructure Coordinating Center Records System of Records." This system of records will allow the Department of Homeland Security National Protection and Programs Directorate National Infrastructure Coordinating Center, an extension of the National Operations Center, to collect, plan, coordinate, report, analyze, and fuse infrastructure information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the National Infrastructure Coordinating Center. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the Federal Register. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before December 15, 2010. This new system will be effective December 15, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS–2010–0086 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: For general questions please contact: Emily Andrew (703–235–2182), Privacy Officer, National Protection and Programs Directorate, Department of Homeland Security, Washington, DC 20528. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) proposes to establish a new DHS system of records titled, "DHS/NPPD–001 National Infrastructure Coordinating Center (NICC) Records System of Records."

This system of records will allow DHS/NPPD, including the NICC (an extension of the National Operations Center (NOC)) to collect, plan, coordinate, report, analyze, and fuse infrastructure information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from Federal, State, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the NICC.

The NICC provides the mission and capabilities to assess the operational status of the nation's 18 critical infrastructures and key resources (CIKR) sectors during normal operations and incident management activities, supports information sharing with National Infrastructure Protection Plan (NIPP) partners, and owners and operators of critical infrastructure facilities, and facilitates information sharing across and between the 18 national sectors.

The NICC is both an operational component of the NPPD Office of Infrastructure Protection (IP) and a watch operations element of the DHS NOC. The NICC operates 24 hours a day, 7 days a week, 365 days a year to facilitate coordination and information sharing with the CIKR sectors. The NICC produces consolidated CIKR reports for incorporation into situational awareness reports and for inclusion into the common operating picture.

DHS is authorized to implement this program primarily through the Homeland Security Act of 2002 as codified within 6 U.S.C. 321d(b)(1), 515. This system has an effect on individual privacy that is balanced by the need to collect, plan, coordinate, report, analyze, and fuse CIKR information coming into and going out of the NICC as well as the NOC. Routine uses contained in this notice include sharing with the Department of Justice (DOJ) for legal advice and representation; to a congressional office at the request of an individual; to the National Archives and Records Administration (NARA) for records management; to contractors in support of their contract assignment to DHS; to appropriate Federal, State, tribal, local, international, foreign agency, or other appropriate entity including the private sector in their role aiding the NICC in their mission; to agencies, organizations or individuals for the purpose of an audit; to agencies, entities, or persons during a security or information compromise or breach; to an agency, organization, or individual when there could potentially be a risk of harm to an individual; and to the news media in the interest of the public. A review of this system is being conducted to determine if the system of records collects information under the Paperwork Reduction Act (PRA).

Based on the information contained within this system of records, the NICC develops reports that are shared both within DHS and with the CIKR sectors. The NICC creates two reports, one with PII and one without. The one without PII is what is shared broadly with the CIKR sectors as well as the state and local fusion centers. Consistent with DHS's information sharing mission, information contained in the DHS/NPPD–001 NICC Records System of Records may be shared with other DHS components, as well as appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a verifiable 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.

The information within this system that meets the functional standard of the National Suspicious Activity Reporting Initiative will be placed into the DHS/ALL–031 Information Sharing Environment Suspicious Activity Reporting Initiative (September 10, 2010, 75 FR 55335).

DHS is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register.** This newly established system will be included in DHS' 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 individuals' records. 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 lawful 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 their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/NPPD—001NICC Records System of Records.

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

System of Records

DHS/NPPD—001

SYSTEM NAME:

DHS/NPPD—001 NICC Records System of Records.

SECURITY CLASSIFICATION:

Unclassified, For Official Use Only, Law Enforcement Sensitive, and Classified.

SYSTEM LOCATION:

Records are maintained at the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) National Infrastructure Coordinating Center (NICC) Headquarters in Washington, DC and field locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by the system may include:

- Federal, State, local, tribal, and territorial officials; foreign government and international officials; domestic security and emergency management officials; and private sector individuals who request assistance from, provide information to, are the subject of, or participate with the NICC in activities related to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters related to national infrastructure;
- Individuals who request assistance from the NICC related to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters related to national infrastructure;
- Individuals who provide information to the NICC related to all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters, including Suspicious Activity Reports (SARs) related to national infrastructure;
- Individuals who are the subject of, or are linked in any manner to, all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters with NICC implications;
- Individuals participating with, involved in, or the subject of domestic security or law enforcement operations, with NICC implications, where activity is planned or has taken place;
- Individuals participating with or involved in emergency management and first responder operations, with NICC, and where activity is planned or has taken place;
- Individuals involved in natural disasters where activity is planned or has taken place;
- Individuals derived from intelligence information of interest to the NICC; and
- Individuals who make inquiries concerning all-threats and all-hazards, man-made disasters and acts of terrorism, and natural disasters related to national infrastructure.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in the system may include:

- Full name;
- Date and place of birth;
- Social Security Number (Many state, local, tribal, territorial, domestic security, emergency management, and private sector individuals, organizations and agencies collect/use SSNs as an identifier and may be shared with the Department);
- Citizenship;
- Contact information including phone numbers and email addresses;
- Address;
- Physical description including height, weight, eye and hair color;
- Distinguishing marks including scars, marks, and tattoos;
- Automobile registration information;
- Watch list information;
- Medical records;
- Financial information;
- Results of intelligence analysis and reporting;
- Ongoing law enforcement investigative information;
- Historical law enforcement information;
- Information systems security analysis and reporting;
- Public source data including commercial databases, media, newspapers, and broadcast transcripts;
- Intelligence information including links to terrorism, law enforcement and any criminal and/or incident activity, and the date information is submitted;
- Intelligence and law enforcement information obtained from federal, state, local, tribal, and territorial agencies and organizations, foreign governments and international organizations; law enforcement, domestic security and emergency management officials; and private sector entities or individuals;
- Information provided by individuals, regardless of the medium, used to submit the information;
- Information obtained from the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC), or on terrorist watchlists, about individuals known or reasonably suspected to be engaged in conduct constituting, preparing for, aiding, or relating to terrorism;
- Data about the providers of information, including the means of transmission of the data; (*e.g.* where it is determined that maintaining the identity of the source of investigative lead information may be necessary to provide an indicator of the reliability and validity of the data provided and to support follow-on investigative purposes relevant and necessary to a legitimate law enforcement or homeland security matter, such data may likely warrant retention. Absent such a need, no information on the provider of the information would be maintained)
- Scope of terrorist, law enforcement, or natural threats to the homeland;
- National disaster threat and activity information;
- The date and time national disaster information is submitted, and the name of the contributing/submitting individual or agency;
- Limited data concerning the providers of information, including the means of transmission of the data may also be retained where necessary. Such information on other than criminal suspects or subjects is accepted and maintained only to the extent that the information provides descriptive matters relevant to a criminal subject or organization and has been deemed factually accurate and relevant to ongoing homeland security situational awareness and monitoring efforts.
- Name of the contributing or submitting agency, organization, or individual.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Homeland Security Act of 2002 as codified within 6 U.S.C. 321d(b)(1), 515 provides DHS, including the NICC and NOC, with authority to collect the information.

PURPOSE(S):

The purpose of this system is to provide the mission and capabilities to assess the operational status of the nation's 18 critical infrastructures and key resources (CIKR) sectors during normal operations and incident management activities, support information sharing with NIPP Partners, and the owners and operators of critical infrastructure.

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 it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

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 the 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 appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations or critical infrastructure partners 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 threat or risk.

I. To a Federal, State, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

J. To Federal and foreign government intelligence or counterterrorism agencies or state, local, tribal or territorial components, and critical infrastructure partners where DHS becomes aware of an indication of a threat or potential threat to national or international security.

K. To Federal and foreign government intelligence or counterterrorism agencies or state, local, tribal or territorial components, and critical infrastructure partners where the information is or may be terrorism-related information and such use is to assist in anti-terrorism efforts.

L. To an organization or individual in either the public or private sector, 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.

M. 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' 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 records are stored on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Much of the data within this system does not pertain to an individual; rather, the information pertains to locations, geographic areas, facilities, and other things or objects not related to individuals. However, some personal information is captured. Personal data may be retrieved by name, Social Security number and other identifiers listed under the Categories of Records Section.

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.

RETENTION AND DISPOSAL:

The NICC is working with the NPPD and DHS Records Officer to develop a NARA approved retention schedule.

SYSTEM MANAGER AND ADDRESS:

Director, National Infrastructure Coordinating Center, Department of Homeland Security, Washington, DC 20528.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security is proposing to exempt this system from the notification, access, and amendment procedures of the Privacy Act. However, DHS/NPPD will consider individual requests to determine whether or not information may be released. 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 NPPD FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under "contacts."

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 Chief Privacy Officer and Chief Freedom of Information Act Officer, *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; and
- 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) may 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 contained in this system is obtained from subject individuals, other Federal, State, local and tribal agencies and organizations, domestic and foreign media, including periodicals, newspapers, and broadcast transcripts, public and classified data systems, reporting individuals, intelligence source documents, investigative reports, and correspondence.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3).

Dated: November 5, 2010.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–28588 Filed 11–12–10; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–5376–N–107]

Notice of Submission of Proposed Information Collection to OMB; Emergency Comment Request; Federal Housing Administration (FHA): Home Energy Retrofit Loan Pilot Program; Notice of Proposed Information Collection for Public Comment

AGENCY: Office of the Chief Information Officer, HUD.

ACTION: Notice of proposed information collection.

SUMMARY: The proposed information collection requirement described below has been submitted to the Office of Management and Budget (OMB) for emergency review and approval, as required by the Paperwork Reduction Act. The Department is soliciting public comments on the subject proposal.

DATES: *Comments Due Date:* November 15, 2010.

ADDRESSES: Interested persons are invited to submit comments regarding this proposal. Comments must be received within zero (0) days from the date of this Notice. Comments should refer to the proposal by name/or OMB approval number) and should be sent to: Ross A. Rutledge, HUD Desk Officer, Office of Management and Budget, New Executive Office Building, Washington, DC 20503; e-mail: *Ross.A.Rutledge@omb.eop.gov*; fax: 202–395–3086.

FOR FURTHER INFORMATION CONTACT: Colette Pollard, Reports Management Officer, QDAM, Department of Housing and Urban Development, 4517th Street, SW., Washington, DC 20410; e-mail *Colette.Pollard@HUD.gov*; telephone 202–402–3400. This is not a toll-free number. Copies of available documents submitted to OMB may be obtained from Ms. Pollard.

SUPPLEMENTARY INFORMATION: This Notice informs the public that the U.S. Department of Housing and Urban Development (HUD) has submitted to OMB, for emergency processing, an information collection package with respect to implementing an FHA Energy Efficient Mortgage Innovation pilot program targeted to the single family housing market. The Consolidated Appropriations Act, 2010 (Pub. L. 111–117, approved December 16, 2009, 123 Stat. 3034) (2010 Appropriations Act), which appropriated fiscal year 2010 funds for HUD, among other agencies, appropriated $50 million for an Energy Innovation Fund to enable HUD to catalyze innovations in the residential energy efficiency sector that have the promise of replicability and help create a standardized home energy efficient retrofit market. Of the $50 million appropriated for the Energy Innovation Fund, the 2010 Appropriations Act stated that "$25,000,000 shall be for the Energy Efficient Mortgage Innovation pilot program directed at the single family housing market." (*See* Pub. L. 111–117, at 123 Stat. 3089). The FHA Home Energy Retrofit Loan Pilot Program (Retrofit Pilot Program) is designed by HUD to meet this statutory directive and provides funding to support that effort. Under the Retrofit Pilot Program, HUD, through FHA-approved lenders, will insure loans for homeowners who are seeking to make energy improvements to their homes.

Lender participation in the Retrofit Pilot Program is voluntary. To facilitate HUD's evaluation of lender performance and assessment of the success and replicability of the pilot program, HUD will select lenders to participate in the program. To be eligible for participation, lenders must submit an Expression of Interest that demonstrates the eligibility of the lender to participate in the Retrofit Pilot Program.

This Notice is soliciting comments from members of the public and affecting agencies concerning the proposed collection of information to: (1) Evaluate whether the proposed