PIA for IECGP

Greene, Sherina

From: VandeSteeg, Sarah
Sent: Friday, November 13, 2009 10:08 AM
To: Greene, Sherina
Subject: RE: Grant Programs Privacy Threshold Analysis (PTAs) for Review

Sorry,

DHS Privacy approved the PTA and determined that FEMA Grants PIA and the DHS/FEMA-004 Grant Management Information Files SORN covers this program.

From: Greene, Sherina
Sent: Friday, November 13, 2009 10:06 AM
To: VandeSteeg, Sarah
Subject: RE: Grant Programs Privacy Threshold Analysis (PTAs) for Review

Question: When you say that the IECGP PTA was approved – meaning approved by whom? FEMA's Privacy Office. Just clarifying.

From: VandeSteeg, Sarah
Sent: Friday, November 13, 2009 9:33 AM
To: Greene, Sherina
Subject: RE: Grant Programs Privacy Threshold Analysis (PTAs) for Review

Good Morning Sherina,

IECGP was approved yesterday. I have attached a copy of the PTA for your records. NSGP is close to being approved. As for the others I will get on them right away.

From: Greene, Sherina
Sent: Friday, November 13, 2009 9:18 AM
To: VandeSteeg, Sarah; Moglia, Dena
Subject: Grant Programs Privacy Threshold Analysis (PTAs) for Review
Importance: High

Hi Sarah and Dena,

I wasn't sure if I sent these PTAs to you for review. Please review the following PTA's for each grant program:

Urban Area Security Initiative Nonprofit Security Grant Program (NSGP)
Driver's License Security Grant Program (DLSGP)
Operation Stonegarden (OPSG)
Buffer Zone Protection Program (BZPP)
Emergency Management Performance Grant (EMPG) Program
Transit Security Grant Program (TSGP)
Interoperable Emergency Communications Grant Program (IECGP)

Please note that these are the PTAs that I have on file and some of the information may need to be updated. If you need additional information please reach out to the poc (Dena Moglia) for more info.

Dena: Can you please send Sarah a PTA for the **Homeland Security Grant Program (HSGP)**? I do not have one for this program on file. I checked the HSGP PRA Package that was sent on 8-27-09 and it was not attached.

Sarah: I believe that the PIA for the Port Security Grant Program (PSGP) was approved by DHS on 7-14-09. Can you please confirm this for me?

Thanks for your help.

Sherina M. Greene
Management Analyst
Collections and Research Branch
Federal Emergency Management Agency
Department of Homeland Security
MD-BO-RM
500 C Street, SW
Washington, DC 20472
Mail Drop Room 3005
1800 South Bell Street
Arlington, VA 22202

"FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards."

IECGP is under this SORN

are suitable for detecting melamine contamination in at-risk components down to 2.5 parts per million (ppm) to give a high degree of assurance that they are not contaminated. At this time, FDA has not established an appropriate level of melamine in drug products.

As explained in detail in the guidance, there have been repeated instances of melamine contamination in food articles, including in the U.S. market. In 2007, FDA learned that certain pet foods were sickening and killing cats and dogs. In September 2008, FDA received reports of melamine-contaminated infant formula in China. These two incidents share the following similarities:

- Melamine, a nitrogen-based compound, was apparently added to bolster the apparent protein content in foods or in ingredients used in processed food products intended to contain protein.
- The recipients of the ingredients using a test for nitrogen content would not have been able to distinguish between melamine and the desired protein.
- Melamine contamination became public only after numerous adverse health events, including deaths, were reported and associated with the use of contaminated products.

These incidents illustrate the potential for drug components to be contaminated with melamine; therefore, it is important for drug manufacturers to be diligent in assuring that no component used in the manufacture of any drug is contaminated with melamine. As of the date of this guidance, FDA is not aware of any pharmaceuticals that are contaminated with melamine. However, because of the potential risk of drug contamination, it is important that manufacturers take steps to ensure that susceptible components are not contaminated with melamine.

We are issuing this level 1 guidance for immediate implementation, consistent with FDA's good guidance practices regulation (21 CFR 10.115). The agency is not seeking comment before implementing this guidance because of the potential for a serious public health impact if melamine-contaminated pharmaceuticals were to enter the domestic market. The guidance represents the agency's current thinking on this issue. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statutes and regulations.

II. Comments

Interested persons may submit to the Division of Dockets Management (see **ADDRESSES**) written or electronic comments regarding this document. Submit a single copy of electronic comments or two paper copies of any mailed comments, except that individuals may submit one paper copy. Comments are to be identified with the docket number found in brackets in the heading of this document. Received comments may be seen in the Division of Dockets Management between 9 a.m. and 4 p.m., Monday through Friday.

III. Electronic Access

Persons with access to the Internet may obtain the document at *http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/default.htm*, *http://www.fda.gov/AnimalVeterinary/GuidanceComplianceEnforcement/GuidanceforIndustry/default.htm*, or *http://www.regulations.gov*.

Dated: July 31, 2009.

Jeffrey Shuren,

Associate Commissioner for Policy and Planning.

[FR Doc. E9–18952 Filed 8–6–09; 8:45 am]

BILLING CODE 4160–01–S

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute of Environmental Health Sciences; Notice of Closed Meeting

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: Environmental Health Sciences Review Committee.

Date: August 25–26, 2009.

Time: 8:30 a.m. to 5 p.m.

Agenda: To review and evaluate grant applications.

Place: Sheraton Chapel Hill Hotel, One Europa Drive, Chapel Hill, NC 27517.

Contact Person: Linda K Bass, PhD, Scientific Review Administrator, Scientific Review Branch, Division of Extramural Research and Training, Nat'l Institute of Environmental Health Sciences, P.O. Box 12233, MD EC–30, Research Triangle Park, NC 27709, (919) 541–1307.

(Catalogue of Federal Domestic Assistance Program Nos. 93.115, Biometry and Risk Estimation—Health Risks from Environmental Exposures; 93.142, NIEHS Hazardous Waste Worker Health and Safety Training; 93.143, NIEHS Superfund Hazardous Substances—Basic Research and Education; 93.894, Resources and Manpower Development in the Environmental Health Sciences; 93.113, Biological Response to Environmental Health Hazards; 93.114, Applied Toxicological Research and Testing, National Institutes of Health, HHS)

Dated: August 3, 2009.

Jennifer Spaeth,

Director, Office of Federal Advisory Committee Policy.

[FR Doc. E9–18993 Filed 8–6–09; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket Number DHS–2008–0159]

Privacy Act of 1974; DHS/FEMA–004 Grant Management Information Files 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 consolidate into one new system its inventory of record systems entitled, Federal Emergency Management Agency Grant Management Information Files. This system will enable the Department of Homeland Security to better administer the Federal Emergency Management Agency Disaster Recovery Assistance Program. Many Federal Emergency Management Agency grant programs collect a minimum amount of contact and grant project proposal information. The information contained in the Federal Emergency Management Agency's Grant Management Information Files is collected in order to determine awards for both disaster and non disaster grants and for the issuance of awarded funds.

DATES: The established system of records will be effective September 8, 2009. Written comments must be submitted on or before September 8, 2009.

ADDRESSES: You may submit comments, identified by DHS–2008–0159 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, such as email address, 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: Alisa Turner (202–646–3102), Branch Chief, Disclosure Office, Federal Emergency Management Agency, Washington, DC 20472. For privacy issues please contact: 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 goal of FEMA's grant programs is to provide funding to enhance the capacity of state and local jurisdictions to prevent, respond to, and recover from disaster and non disaster incidents including cyber attacks. FEMA's grant programs currently provide funds to all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of Northern Mariana Islands, Guam, and the U.S. Virgin Islands. FEMA grant programs are directed at a broad spectrum of state and local emergency responders, including firefighters, emergency medical services, emergency management agencies, law enforcement, and public officials. The source of the information that FEMA is collecting generally comes from state, local, and tribal partners seeking grant funding. Additional sources of information may include private and non private organizations. The nature of the collected data should illustrate organizations' familiarity with the national preparedness architecture (i.e. Federal Investment Strategy), identify how elements of this architecture have been incorporated into their regional/state/local planning, operations, and investments, and the demonstrated need for the grant funds.

Many of FEMA's grant programs implement objectives addressed in a series of post-9/11 laws, strategy documents, plans, and Homeland Security Presidential Directives (HSPDs). FEMA management requirements are incorporated into the application processes and reflect changes mandated in the Implementing Recommendations of the 9/11 Commission Act of 2007 (the "9/11 Act"), enacted in August 2007, as well as the FY 2008 Consolidated Appropriations Act.

Consistent with DHS's information sharing mission, information stored in the Grants Management Information Files may be shared with other DHS components, as well as appropriate federal, state, local, tribal, foreign, or international government agencies. This sharing will take place only 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.

The information contained in the FEMA Grant Management Information Files is collected in order to determine awards for both disaster and non-disaster grants and for the issuance of awarded funds.

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 FEMA Grants Management Information Files 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/FEMA–004

SYSTEM NAME:

DHS/FEMA–004 Grant Management Information Files.

SECURITY CLASSIFICATION:

Unclassified and sensitive.

SYSTEM LOCATION:

Records are maintained at Federal Emergency Management Agency Headquarters in Washington, DC and field offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of entities covered by this system include: Recipients (grantees) of grant funds. These include state, territorial, tribal officials, port authorities, transit authorities, non-profit organizations, and, in rare instances, private companies.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Organizational Name;
- Employer Identification Number (EIN);
- Name of Organization's Designated Point of Contact (POC);
- POC work address;
- POC work phone number;
- POC cellphone number;
- POC fax number;
- POC work e-mail address;
- Organization's Bank Routing Number;
- Organization's Bank Account Number; and
- Grant related information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Legal authority includes, but is not limited to:

- The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5133

- The National Flood Insurance Act, 42 U.S.C. 4104c
- Section 2003(a) of the Homeland Security Act of 2002 (6 U.S.C. 101 *et seq.*), as amended by Section 101, Title I of the Implementing Recommendations of the 9/11 Commission Act of 2007, (Pub. L. 110–053)
- Section 2004(a) of the Homeland Security Act of 2002 (6 U.S.C. 101 *et seq.*), as amended by Section 101, Title I of the Implementing Recommendations of the 9/11 Commission Act of 2007, (Pub. L. 110–053)
- Section 1809 of the Homeland Security Act of 2002 (6 U.S.C. 571 *et seq.*), as amended by Section 301(a), Title III of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–053)
- The Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 723)
- Title III of Division D of the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (Pub. L. 110–329)
- Section 614 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196c), as amended by Section 202, Title II of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–053)
- Title III of Division E of the Consolidated Appropriations Act, 2008 (Pub. L. 110–161)
- Section 1406, Title XIV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–053)
- Section 1513, Title XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–053)
- Section 1532(a), Title XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–053)
- 46 U.S.C. 70107
- Federal Financial Assistance Management Improvement Act of 1999 (Pub. L. 106–107)

PURPOSE(S):

The purpose of this system is to assist in determining awards for both disaster and non-disaster grants and for the issuance of awarded funds and allow DHS to contact individuals to ensure completeness and accuracy of grants and applications.

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 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) 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 an individual's employer or affiliated organization to the extent necessary to verify employment or membership status.

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

RETRIEVABILITY:

Records may be retrieved by name of organization or contact person covered by this system.

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. Additional safeguards may vary by component and program.

RETENTION AND DISPOSAL:

In accordance with the Federal records retention requirements, Grant administrative records and hard copies of unsuccessful grant applications files are destroyed when two years old (Government Records Schedule (GRS) No. 3, Procurement, Supply, and Grant Records, Item 14). Electronically received and processed copies of unsuccessful grant application files are destroyed three years after rejection or withdrawal (GRS No. 3, Procurement, Supply, and Grant Records, Item 13). Grant Project Records are maintained for three years after the end of the fiscal year that the grant or agreement is finalized or when no longer needed, whichever is sooner. These records are disposed of IAW FEMA Records Schedule N1–311–95–1, Item 1. Grant Final Reports are retired to the Federal Records Center three years after cutoff, and then transferred to National Archives 20 years after cutoff. These records are maintained IAW FEMA Records Schedule N1–311–95–1, Item 3. All other grant (both disaster and non disaster) records are maintained for six years and three months after the end of the fiscal year when grant or agreement is completed or closed. These records are disposed of according to IAW FEMA Records Schedule N1–311–95–1, Item 2; N1–311–01–8, Item 1; and N1–311–04–1, Item 1.

SYSTEM MANAGER AND ADDRESS:

Deputy Assistant Administrator, Grant Program Directorate, FEMA, 500 C Street, SW., Washington, DC 20472.

NOTIFICATION PROCEDURE:

Individuals or entities 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., STOP–0655, 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:

Records are obtained by grantees, applicants for award, and grant program monitors.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: July 31, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–18931 Filed 8–6–09; 8:45 am]

BILLING CODE 9110–17–P

DEPARTMENT OF THE INTERIOR

Bureau of Indian Affairs

Class III Gaming; Tribal Revenue Allocation Plans; Gaming on Trust Lands

AGENCY: Bureau of Indian Affairs, Interior.

ACTION: Notice of submission of information collection renewal to the Office of Management and Budget.

SUMMARY: In compliance with the Paperwork Reduction Act, the Bureau of Indian Affairs (BIA) is submitting the following information collections to the Office of Management and Budget (OMB) for renewal: Class III Gaming Procedures 25 CFR 291, 1076–0149; Tribal Revenue Allocation Plans 25 CFR 290, 1076–0152; and Gaming On Trust Lands Acquired After October 17, 1988, 25 CFR 292, 1076–0158. The current approvals for the first two collections (1076–1049 and 1076–0152) expire August 31, 2009 and the current approval for the third collection (1076–0158) expires February 28, 2010. Renewal will allow us to continue to collect the information necessary to comply with the Indian Gaming Regulatory Act (IGRA).

DATES: Submit comments on or before September 8, 2009.

ADDRESSES: Submit comments on the information collection to the Desk Officer for the Department of the Interior, OIRA, Office of Management and Budget, by fax at (202) 395–5806 or e-mail at *OIRA_DOCKET@ omb.eop.gov.*

Please send a copy of your comments to: Paula L. Hart, Office of Indian Gaming, Mail Stop 3657–MIB, 1849 C Street, NW., Washington, DC 20240, Facsimile: (202) 273–3153.

FOR FURTHER INFORMATION CONTACT: You may request further information or obtain copies of the proposed information collection request from Paula L. Hart, Telephone: (202) 219–4066.

SUPPLEMENTARY INFORMATION:

I. Abstract

This information collection is necessary for the BIA, Office of Indian Gaming, to ensure that the applicable requirements for IGRA, 25 U.S.C. 2701

Privacy Impact Assessment
for the

Grant Management Programs

July 14, 2009

Contact Point
Tracey Trautman
Deputy Assistant Administrator
Grant Programs Directorate
(202) 786-9730

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

Many of the Department of Homeland Security Federal Emergency Management Agency (FEMA) grant operations and projects collect a minimum amount of contact information. The information is collected in order to determine awards for both disaster and non-disaster grants and for the issuance of awarded funds. This Privacy Impact Assessment (PIA) is conducted because the information provided by applicants includes personal identifiable information (PII).

Overview

The primary mission of the Federal Emergency Management Agency (FEMA) is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters, by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation. One of FEMA's objectives is to prepare America for these hazards by developing and implementing national programs to enhance the capacity of state, local, and tribal government agencies to respond to these incidents through coordinated training, equipment acquisition, technical assistance, and support for Federal, state, and local exercises. FEMA fulfills this mission through a series of grant programs responsive to the specific requirements of state, local agencies.

The goal of FEMA's grant programs is to provide funding to enhance the capacity of state and local jurisdictions to prevent, respond to, and recover from disaster and non disaster incidents including cyber attacks. FEMA's grant programs currently provide funds to all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of Northern Mariana Islands, Guam, and the U.S. Virgin Islands. FEMA grant programs are directed at a broad spectrum of state and local emergency responders, including firefighters, emergency medical services, emergency management agencies, law enforcement, and public officials. FEMA is collecting information from State, local, and tribal partners seeking grant funding. The nature of the collected data should illustrate partners' familiarity with the national preparedness architecture (i.e. Federal Investment Strategy) and identify how elements of this architecture have been incorporated into their regional/state/local planning, operations, and investments.

Many of FEMA's grant programs implement objectives addressed in a series of post-9/11 laws, strategy documents, plans and Homeland Security Presidential Directives (HSPDs). FEMA management requirements are incorporated into the application processes and reflect changes mandated in the Implementing Recommendations of the 9/11 Commission Act of 2007 (the "9/11 Act"), enacted in August 2007, as well as the FY 2008 Consolidated Appropriations Act.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Applications submitted for FEMA grants generally include information about the applying agency or organization, including the name of the organization point of contact for the application, work address, work phone and fax numbers, cell phone number, and work email address. Information for grant processing also includes the organizations' Federal Employer Identification Number (EIN) information about the activity or activities proposed to be completed under the requested grant as well as banking information such as bank account number and routing number. Generally, the only sensitive PII FEMA may collect as part of the grants is the social security number used as EIN for small businesses and organizations. In instances where grants may require such collections DHS/FEMA will conduct a separate PIA analyzing the risks associated with such sensitive collections.

1.2 What are the sources of the information in the system?

Information is collected from state/territorial/tribal officials, port authorities, transit authorities, non-profit organizations, and, in rare instances, private companies. The information is entered into Grants.gov.

1.3 Why is the information being collected, used, disseminated, or maintained?

Contact information such as the organization's POC name, contact number, and addresses (mailing and email) is collected to facilitate on-going communications with the applicants via e-mail, telephone, and postal mail. Financial information is collected for the transfer of funds provided under a FEMA disaster or non disaster grant. Project proposal information is collected to inform the peer review decision-making process in relation to application completeness, adherence to programmatic guidelines, feasibility, and how well the proposed investments address identified need(s) or capability shortfall(s).

1.4 How is the information collected?

Information is collected generally via online application, but occasionally by telephone inquiries or paper forms.

1.5 How will the information be checked for accuracy?

Information is collected directly from individuals and is assumed to be accurate. Depending on the

nature of the grant (disaster or non disaster) and the grant program, the project or program may conduct a certain degree of verification of information and follow up with the organization's point of contact.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The legal authorities that govern FEMA's collection of information regarding its grant programs include, but are not limited to, the following:

- The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5133
- The National Flood Insurance Act, 42 U.S.C. 4104c
- Section 2003(a) of the Homeland Security Act of 2002 (6 USC §101 et seq.), as amended by Section 101, Title I of the Implementing Recommendations of the 9/11 Commission Act of 2007, (P.L. 110-053)
- Section 2004(a) of the Homeland Security Act of 2002 (6 USC §101 et seq.), as amended by Section 101, Title I of the Implementing Recommendations of the 9/11 Commission Act of 2007, (P.L. 110-053)
- Section 1809 of the Homeland Security Act of 2002 (6 USC §571 et seq.), as amended by Section 301(a), Title III of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-053)
- Post-Katrina Emergency Management Reform Act of 2006 (6 USC §723).
- by Title III of Division D of the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (P.L. 110-329)
- Section 614 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 USC §5196c), as amended by Section 202, Title II of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-053)
- Title III of Division E of the Consolidated Appropriations Act, 2008 (P.L. 110-161)
- Section 1406, Title XIV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-053)
- Section 1513, Title XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-053)
- Section 1532(a), Title XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-053)
- 46 USC §70107
- Federal Financial Assistance Management Improvement Act of 1999 (P.L.106-107).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The privacy risk presented by a basic contact list is that more information will be collected than is necessary to distribute information. Contact information is limited to the information necessary to perform the information distribution functions of the program or project. All information is collected with the consent of the individual.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

FEMA uses the information to determine grant eligibility, to contact an applicant, to transfer funds to the grant awardee(s) in accord with the grant awarded, and to inform the peer review panel in determining how well proposed investments address identified homeland security need(s) or capability shortfall(s).

Additionally, FEMA uses the information to generate reports summarizing grant activity of applicant organizations. These reports are used to assist in the management and reporting of grant programs including overall Grants Management, Program-Specific Progress, Functions and Monitoring, Financial Management, management of Grantee and Sub-Grantee data (if available), System Administration, and Common Services.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Information is stored but is not manipulated in any way other than to, if necessary, generate summary reports about grants for specific applicant organizations. Summary reports will not be generated by individual's name or any other identifier. Data may be input into databases or electronic spreadsheets and accessed via the various data elements. For example, a query may be conducted to calculate total grant funds obligated within a certain state or a list of all grants awarded in a certain state.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Grant applications are not created, populated with, or verified with data collected from commercial or publicly available sources.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The risk presented by the use of contact information or project proposal information is that the information would be used in ways outside the scope intended by the initial collection. Per the Grants Management Information Files System of Records Notice (SORN) and the Privacy Act Statements given prior to collection, information collected is not to be used for any purpose other than what has been stated and communicated. Additionally, all Department employees and contractors are trained on the appropriate use of this sensitive information and are required to obtain the appropriate level of security clearance to handle certain data.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

All information provided by the grant applicant as outlined in section 1.1 and 1.3 of this PIA is retained in each grant applicants file (paper and or electronic).

3.2 How long is information retained?

In accordance with the Federal records retention requirements, Grant administrative records and hard copies of unsuccessful grant applications files are destroyed when two years old (Government Records Schedule (GRS) No. 3, Procurement, Supply, and Grant Records, Item 14). Electronically received and processed copies of unsuccessful grant application files are destroyed three years after rejection or withdrawal (GRS No. 3, Procurement, Supply, and Grant Records, Item 13). Grant Project Records are maintained for three years after the end of the fiscal year that the grant or agreement is finalized or when no longer needed, whichever is sooner. These records are disposed of IAW FEMA Records Schedule N1-311-95-1, Item 1. Grant Final Reports are retired to the Federal Records Center three years after cutoff, and then transferred to National Archives 20 years after cutoff. These records are maintained IAW FEMA Records Schedule N1-311-95-1, Item 3. All other grant (both disaster and non-disaster) records are maintained for six years and three months after the end of the fiscal year when grant or agreement is completed or closed. These records are disposed of according to IAW FEMA Records Schedule N1-311-95-1, Item 2; N1-311-01-8, Item 1; and N1-311-04-1, Item 1.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Records are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 3, Procurement, Supply, and Grant Records, Items 13 and 14. Additionally, grant files are under record group 311 and individual files generated are covered by FEMA File Numbers PRC-12 through PRC-13-4. These record retentions have been approved by the NARA (Job Numbers N1-311-01-8, N1-311-04-1, and N1-311-95-1) and are published in FEMA Manual 5400-2M, dated February 2000.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Information other than grant final reports is retained for no more than six years and three months after the grant is closed and final audit and appeals are resolved and completed. Grant final reports, which generally do not contain sensitive information, will be maintained at secured federal locations. This

minimizes retention and security costs associated with maintaining contact, financial, and project information.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Grant application information may be shared with internal DHS components inasmuch as they are involved in distributing information or collaborating with partners within the Department and within the Nation's homeland security community. However, DHS does not share contact information for any purpose beyond which it was originally collected, i.e. contact information given by organizations for purpose *x* will not be shared for use of purpose *y* at a later date.

4.2 How is the information transmitted or disclosed?

FEMA may share information by electronic or paper means. If information is transmitted electronically, proper security measures are taken, including encryption and/or use of Sensitive Compartmented Information Facilities (SCIFs) when necessary. For example, information may be transmitted via an authenticated web interface, and regulated via role based access controls. Information access is limited to the minimum necessary to perform required job functions.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Inappropriate sharing is a risk inherent in any collection of sensitive information. Department employees and contractors are trained on the appropriate use and sharing of sensitive information and are required to obtain the appropriate level of security clearance to handle certain data. Further, any sharing of information must align with the purpose of the initial collection as described in its SORN and include the Privacy Act Statement provided at the time of collection.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Contact and project information may be shared with external homeland security entities inasmuch as those entities are involved in distributing information or collaborating with partners within FEMA, DHS, and homeland security officials throughout the Nation. Nonetheless, sensitive information is not shared for any purpose beyond which it was originally collected, i.e. contact information given by individuals for purpose x will not be shared for use of purpose y at a later date.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. Per the Grants Management Information Files SORN and the various notices provided when information is collected, use of application information beyond the purposes for which it was originally collected is not acceptable.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Any information shared with organizations outside the Department is required to be appropriately secured per Office of Management and Budget Memoranda 06-15, Safeguarding Personally Identifiable Information, and 06-16, Protection of Sensitive Agency Information.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

A risk is presented whenever FEMA shares information it has initially collected from organizations or individuals outside of the Department. If external sharing of information would exceed the purpose for which the information was collected, then the information is not permitted to be shared. The Grants Management Information Files SORN outlines the specific instances where contact and project proposal information may be shared outside the Department. All FEMA employees and contractors receive training

on the appropriate use and sharing of information and are required to obtain the appropriate level of security clearance to handle certain data.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. This PIA and the Grants Management Information Files SORN provide notice regarding the collection of contact and project proposal information by FEMA. More appropriately, though, each collection of grant information is immediately preceded by notice regarding the scope and purpose of the contact and project proposal information at the time of collection. These Privacy Act Statements (these notices are required under 5 U.S.C. § 552a(e)(3)) at the moment of collection provide individuals and organizations with notice of the nature of the collection and the authority to collect the information.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

No. Applicants are required to provide contact and project proposal information as mandated by law. If requested information is not provided in its entirety, it is likely that applicants will not receive grant funding and will not receive information from the Department or partners in the Department.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

DHS will use the information only for the purposes for which it was collected. Should an organization suspect information is being used beyond the given scope of the collection, they are encouraged to write to FEMA/FOIA, 500 "C" Street, NW, Washington, DC 20472. The system managers are also listed in the Grants Management Information Files SORN.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The privacy risk associated with notice in the collection of contact and project proposal information is that the applicant is not aware of the purpose for which the information he or she submits may be used. This risk is primarily mitigated by limiting the use of application information to what is necessary for the purposes of awarding a grant. Additionally, the Grants Management Information Files SORN provides notice of the purpose of the collection, redress procedures, and the routine uses associated

with the collection of contact information. Notice is always provided prior to the collection of information, and consent is obtained by the organization prior to his providing information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Should an organization seek to update either their grant application or grant they should contact the grant program office or project which initially collected the information. The grant program or project is in the best position to remove, edit and/or provide access to the information held on an organization. Access requests can also be directed to the following: Federal Emergency Management, 500 "C" Street, MS 857, Washington, DC 20472, Attn: FOIA. In the case of a system covered by this PIA, generally, once a request for a grant application has been approved, the specified organizational contact person is provided logon credentials to their account. Once an organization's point of contact is authenticated, they will be able to make changes as allowed by the program and the system.

Additionally, the Grants Management Information Files SORN details access provisions along with the names of officials designated to field such requests within FEMA.

7.2 What are the procedures for correcting inaccurate or erroneous information?

The procedures are the same as those outlined in Question 7.1. The specific grant program office or project that initially collected the information is in the best position to correct or amend any inaccurate or outdated information. Any inquires for correction should be made to the grant program office or project that initially collected the information.

Additionally, the Grants Management Information Files SORN details access provisions along with the names of officials designated to field such requests within FEMA.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are notified at collection that they may amend or correct their information at any time by the procedures outlined above.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Appropriate redress is provided as described in 7.1.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Organizations may amend or correct information at any time during which FEMA possesses and uses their application information. Any risks associated with correction of information are thoroughly mitigated by the organizations' ability to correct its information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

FEMA physical and information security policies dictate who may access FEMA computers and filing systems. Specifically, DHS Management Directive 4300A and FEMA Information Technology Security Policy Directive outline information technology procedures for granting access to DHS/FEMA computers, which is where grant information is stored. Access to application information is strictly limited by access controls to those who require it for completion of their official duties.

8.2 Will Department contractors have access to the system?

Yes, depending on the grant project or program. Many times contractors are tasked with information processing, distribution and other outreach tasks. Contractors are required to have the same level of security clearance in order to access DHS/FEMA computers as all other FEMA employees.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All FEMA employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of sensitive information such as the type of information contained in a grant application submission.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

In compliance with the Federal Information Security Management Act of 2005, systems supporting disaster and non-disaster grants covered by this PIA will go through the Certification and Accreditation process and will be listed in Appendix A.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

All FEMA information systems are audited regularly to ensure appropriate use and access to information. Additionally, grant information residing on a local area network's shared drive is restricted by access controls to those who require it for completion of their official duties. Folders within shared drives are privilege-protected.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk of unauthorized access exists with any information technology system or document. FEMA conducts thorough background checks on every employee and contractor. Access to the systems and networks which store the grant contact and financial information are protected pursuant to established Departmental and Agency procedures (see 8.4).

All FEMA employees and contractors are trained on security procedures, specifically as they relate to sensitive information.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

This assessment covers grant application processes developed by a program or project involved in outreach or collaboration efforts within or outside of DHS.

9.2 What stage of development is the system in and what project development lifecycle was used?

The program or projects detailed here are not necessarily involved in a specific lifecycle. Complete information technology systems are in the operational phase and have completed C&A documentation. Appendix A will list all grant information systems covered by this PIA and its C&A status as well and specific lifecycles used.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

If a particular technology used in the collection or handling of information in connection with the types of contact lists addressed in this PIA raises specific and/or heightened privacy concerns, the implementation of the technology will be required to conduct a separate PIA.

Approval Signature

Original signed and file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A (Grant Programs/Systems covered by this PIA)

Assistance to Firefighters Grant Program

Port Security Grant Program

Non-Disaster Grant System

Grants Reporting Tool