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

Environmental-Historic Preservation Management Information System (EMIS)

Regional Catastrophic Preparedness Grant Program (RCPGP)

Trucking Security Program

Grants Management Integrated Environment (GMIE)