Privacy Impact Assessment
for the

National Emergency Management Information System – Mitigation (MT) Electronic Grants Management System (NEMIS-MT eGrants)

January 19, 2007

Contact Point
Shabbar Saifee
Federal Emergency Management Agency (FEMA)
Mitigation Division
Risk Reduction Branch
Grants Data Analysis & Tools Section

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The Federal Emergency Management Agency (FEMA) operates the National Emergency Management Information System (NEMIS) Mitigation (MT) Electronic Grants Management (eGrants) system. The eGrants system is an online grant application and grant management system. This privacy impact assessment (PIA) is being conducted because personally identifiable information may be included in grant applications made by States or local communities.

Introduction

This PIA addresses all of the Mitigation Division's grant programs that collect applications through MT eGrants. These include the Flood Mitigation Assistance (FMA), Pre-Disaster Mitigation (PDM), Severe Repetitive Loss (SRL), Repetitive Flood Claims (RFC), Hazard Mitigation Grant Program (HMGP), and related mitigation grant programs authorized under either the Robert T. Stafford Disaster Relief and Emergency Assistance Act or the National Flood Insurance Act, 42 U.S.C. 4100.

The purpose of FEMA Mitigation grant programs is to provide funds to eligible States (applicants) and local communities (sub-applicants through State applications) to implement mitigation activities to reduce or eliminate the risk of future damage to life and property.[1] Examples of mitigation activities include retrofitting structures, minor structural flood control projects, acquisition of properties, demolition or relocation of structures, construction of safe rooms, or developing local or statewide mitigation plans.

FEMA is also the administrator of the National Flood Insurance Program (NFIP) (42 U.S.C. § 4001 et seq.), a Federal program enabling property owners in participating communities to purchase insurance as a protection against flood losses in exchange for State and local community floodplain management regulations that reduce future flood damages. Individual properties are included in applications and are verified against NFIP data manually for insurance status and/or damage history prior to any mitigation grant funds awarded. Because States are the lead applicants and local communities are sub-applicants (where sub-applicants exist), the terms "State" and "local community" will hereinafter be used to describe the applicants and sub-applicants, respectively.

The eGrants system is an online grant application and grant management system. Individuals who own property and who may be eligible for FEMA mitigation grants must voluntarily request assistance through their State or local community. Individuals may not apply directly to FEMA and are not granted direct access to the eGrants system. The State or local community collects the individual's information through a paper application, and enters the information into the 'Properties' section of an online grant application.[2] A grant application includes multiple properties and other local community and State-specific information. The State submits the application to FEMA for review and, if approved, the State signs and accepts a grant award. All transactions are completed online and information is secured on FEMA servers.

---

[1] States serve as the primary applicants. Municipalities and/or local communities may serve as sub-applicants. Individual owners never serve as the applicant.

[2] Eligible applicants for FEMA Mitigation grants include only the State emergency management agencies or similar State offices that have emergency management responsibility, including all 50 States, the District of Columbia, the U.S. Virgin Islands, the Commonwealth of Puerto Rico, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, and Federally recognized Indian Tribal governments.

This privacy impact assessment is being conducted because personally identifiable information about property owners may be included in the State or local community's application. While individuals and private, non-profit organizations are not eligible applicants and cannot apply directly to FEMA for assistance, some (but not all) applications may potentially impact properties that are privately owned by individuals (e.g., acquisition of a home that has been repeatedly flooded). These applications include personally identifiable information about the property owners.

Local communities to whom a sub-grant is awarded are accountable to the State for the use of the funds provided. The information collected in e-Grants is provided by the State and any local communities and includes information about the proposed activity or activities to be completed under a grant.

eGrants is composed of an Internet-based program and an Intranet-based program. The information collected in the Internet-based program includes information from eligible States and local communities and is the minimum information needed to determine an State's and local community's eligibility for funding under FEMA Mitigation grant programs.

Section 1.0 Information Collected and Maintained

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

1.1 What information is to be collected?

The personally identifiable information that may be included in an application includes an individual's name, home phone number, office phone number, cell phone number, damaged property address, mailing address of the individual property owner(s), the individual's status of flood insurance, National Flood Insurance Program Policy Number, and the Insurance Policy Provider for the property proposed to be mitigated with FEMA funds.[3]

Additionally, with each application information is provided by the State for point of contact purposes that includes name of the point of contact for the application, work address, work phone number, and work email address. This information is manually verified to determine eligibility for the State.

1.2 From whom is information collected?

The personally identifiable information is collected by FEMA from any State or local community as it may be part of a State's application and also part of a local community's application as a sub-applicant. Local communities may work with individual property owners to apply for a grant that will allow them to voluntarily mitigate their property and may provide personally identifiable information in their sub-application about these individuals.

The sources of the information are the State emergency management agencies or other State offices with emergency management responsibility and federally-recognized Indian Tribal governments who choose to apply to FEMA directly.[4] Local communities to which a sub-grant is awarded are accountable to

[3] Cell phone numbers are an optional field and are indicated as such on the eGrants forms. Phone numbers may be helpful to FEMA or Applicant/States in order to follow up for information regarding an application or more details about a property.
[4] Eligible applicants for FEMA Mitigation grants include only the State emergency management agencies or similar State offices that have emergency

the State for the use of the funds provided. The information collected in eGrants is provided by the State and any local communities and includes information about the proposed activity or activities to be completed under a grant.

The primary source of personally identifiable information is the local communities who obtain personally identifiable information from individual property owners interested in mitigating risks of future damage to their homes and businesses. The individual property owners, after consultation, voluntarily give their personally identifiable information to their local community or Indian tribe who may apply for grants on their behalf.

Local communities may contact individuals directly or individuals may voluntarily contact their local community to express their personal interest in applying for grant funds. Once identified, the local community includes information voluntarily provided by individuals who are property owners in the sub-application, which is submitted to the State and then included in that State's application to FEMA.

1.3 Why is the information being collected?

The information is being collected for the purpose of administering grants programs. Specifically, the information is collected for FEMA to evaluate and determine the eligibility of applicants (both States and local communities as previously defined) and the proposed activities (specifically, those that mitigate individual properties) to be considered for grants funding under FEMA Mitigation grant programs.

1.4 How is the information collected?

Information is collected electronically through the eGrants computer interface.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

This information is necessary for FEMA to determine the eligibility of activities proposed by the State and local community and consequently to allocate FEMA Mitigation funds for eligible, cost-effective mitigation activities, in accordance with the following authorizing legislation:

- Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended by Section 102 of the Disaster Mitigation Act of 2000 (DMA), Public Law 106–390, 114 Stat. §1552. Can be found at http://www.fema.gov/library/viewRecord.do?id=1935.
- National Flood Insurance Act, 42 U.S.C. § 4100, as amended by the Bunning-Bereuter-Blumenauer Flood Insurance Reform Act of 2004, Public Law 108-264, 118 Stat. § 712, and 42 U.S.C. § 4001 et seq., Can be found at http://www.access.gpo.gov/uscode/title42/chapter50_.html.

management responsibility, including all 50 States, the District of Columbia, the U.S. Virgin Islands, the Commonwealth of Puerto Rico, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, and Federally recognized Indian Tribal governments.

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

Personally identifiable information collected in these applications includes the minimum amount necessary for FEMA to ascertain the eligibility of a property and/or structure under the Mitigation grant program regulations. Although FEMA is not the initial collector of the information, FEMA recognizes its duty to protect the personally identifiable information it may come into contact with or maintain in its systems.

Section 2.0 Uses of the System and 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.

The information is used to evaluate and determine the eligibility of States and local communities and the proposed activities (specifically those that mitigate individual properties) to be considered for grants funding under FEMA Mitigation grant programs.

Some (but not all) applications by States and local communities propose activities which would impact properties (e.g., acquisition of a property that has been repeatedly flooded) privately owned by individuals. The information provided in applications is necessary to verify whether a property is eligible for Mitigation grants.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "datamining")?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Information submitted by eligible States is manually checked for accuracy by FEMA. First, the public information about the State, including the name of the point-of-contact for the application, work address, work phone number, and work email address, is manually verified to determine the applicant's eligibility. Second, individual properties that are included in applications are manually verified against NFIP data for insured status and/or damage history prior to award of any Mitigation grant program funds.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Any information that FEMA receives in an application is used for the discrete purpose of verifying eligibility for a grant. Uses of any other kind are specifically prohibited per eGrants system security measures detailed in Section 8. Additionally, FEMA takes great measures in verifying the information it receives by separately and manually verifying public and private information. This ensures that FEMA has accurate information upon which to determine eligibility.

Section 3.0 Retention

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

3.1 What is the retention period for the data in the system?

The data in the system are considered to be federal government records. Pursuant to the Government Paperwork Elimination Act (http://www.whitehouse.gov/omb/fedreg/gpea2.html) and Office of Management and Budget (OMB) Circular A-130, electronic records are given the same validity as paper-based records. Therefore, the retention periods for eGrants data are consistent with retention schedules established by the National Archives and Records Administration (NARA) and the U.S. Department of Treasury. Specifically, for successful applications, the retention schedule is six (6) years, three (3) months after close-out; for unsuccessful applications, the retention schedule is three (3) years from award date.

FEMA's policies and procedures for expunging data, including records pertaining to approved and unapproved grant applications, at the end of retention period are consistent with NARA policy guidance. These procedures are documented by the FEMA Records Officer and follow NARA's general records schedule guidelines, including the submittal of SF 115 forms to NARA. Electronic records are destroyed in accordance to the same NARA records retention schedule as the hard paper copies.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes.

5.1 With which external organizations is the information shared?

The State or local community generally collects the individual's information, inputs the information into the 'Properties' section of the online grant application, and transmits the information to FEMA. The collection of information from individuals may be done on paper or through other means at the State or local level, but must occur prior to FEMA's receipt of the information. Only authorized users of the eGrants system (further described under Section 8.1) are allowed to enter the individual's information into the system. Therefore FEMA shares the information only with such authorized users. The only information shared by FEMA with States or local communities is information that which was originally entered into the system by these eligible States, or by the local community organizations in their respective State, or other eligible applying agency.

Nevertheless, once FEMA receives an application it does not share information outside of FEMA (Section 4.0).

5.2 What information is shared and for what purpose?

The eGrants system contains information submitted by registered State and local community users, described further in Section 8.1. The information is shared by these users with FEMA, and includes personally identifiable information on individual property owners whose properties may be impacted by an activity proposed in an application. The only information shared by FEMA with these other agencies is information that which was originally entered into the system by these eligible State agencies, or by the local community organizations in their respective State or other eligible applying agency.

In the online interface States may input new data or use data they have previously entered to develop new applications. Local communities may input new data or use data they have previously entered to develop and manage sub-applications, including applications for activities to mitigate individuals' properties. States may review sub-applications submitted by local communities, including applications for activities to mitigate individuals' properties. States also submit applications to FEMA and manage the status of submitted applications.

5.3 How is the information transmitted or disclosed?

The information is transmitted by State users to FEMA electronically via the eGrants interface. The 'Properties' section of the application allows information to be imported from spreadsheets (Microsoft Excel), if there are multiple properties being entered into an application. States and local communities are responsible for ensuring that spreadsheets with individuals' information stored on their computers or networks are secure. The eGrants security features described in Section 8.0 are designed to protect the information transferred in the interface and information stored by FEMA.

Once the information is entered and electronically submitted to FEMA, States and local communities may view data via the Internet as explained in Section 8.1. They may use the 'Copy and Paste' functions on their Internet browser to copy data or they may print information from their web browser. Printed or copied information is subject to the same privacy requirements as the eGrants system. There are

no other features in the eGrants system that allows transmittal or disclosure of information to unauthorized users of the system.

Nonetheless, it must be noted that FEMA does not share information once it is received. States and local communities have access to the information they have submitted, but FEMA does not share that information with anyone other than original collectors and submitters.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

FEMA publishes guidance for each of its annual mitigation grant programs detailing the information required for all applications and the required use of eGrants as the official application. This guidance is made available to all States and local communities, and is posted on the FEMA website at http://www.fema.gov. All States and local communities who submit information via the eGrants electronic application are made aware of the Privacy Act requirements via a Privacy Statement on the eGrants interface (Appendix B). In addition, States and local communities are required to provide an e-signature prior to submittal that completes the SF 424, Application for Federal Assistance, that indicates by signing the application they have certified that all statements are true, complete, and accurate to the best of their knowledge (U.S. Code, Title 218, Section 1001).

5.5 How is the shared information secured by the recipient?

Information entered into the eGrants interface resides on FEMA servers, and is therefore secured in accordance with FEMA protocols as described further in Section 8.8. All States and local communities that submit information via the eGrants electronic application are made aware of the Privacy Act requirements via a Privacy Statement in eGrants. Information copied, printed, or otherwise retained by States or local communities are subject to the same requirements for retaining personal information as defined under the eGrants System of Records Notice (SORN).

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Although FEMA does not provide hands on training to States and local communties, the NFIP legislation and eGrants program guidance requires consultation with individuals prior to their involvement in the eGrants process, and requires States and local communities to notify individuals of the voluntary nature of their participation. Question 6.2 provides a more robust response regarding this notice. Once information is submitted to FEMA by eligible States and local communities, FEMA is responsible for assuring proper use of the data by State and local communities.

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

The eGrants interface provides a secure environment for application management between FEMA and the State. FEMA protects the information and the channels through which information is shared. States have access to only the information they have submitted themselves. FEMA does not share application information with any organization other than the State, and the information that is "shared" is only the information that State submits. Risks associated with this information sharing are limited and are mitigated by the access controls detailed in Section 8.0.

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? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Please see the attached Systems of Records Notice for the "NEMIS-MT e-Grants, Mitigation Electronic Grants Management System," Published December 15, 2004 (Appendix A). States and local communities are required to share the SORN with individuals that are included in an application for FEMA mitigation grants.

FEMA posted a Privacy Statement that includes the disclosure of routine uses for FEMA, States and local community users of the eGrants web site (Appendix B). States and local communities who access the eGrants interface to enter information are presented with the Privacy Statement.

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

Yes, in addition to the system of records notice discussed in 6.1, individuals are consulted and informed of the voluntary nature of their participation in the program (i.e., the collection of their information). States and local communities are required by the NFIP and the eGrants program guidance to consult with individuals and obtain their voluntary consent to participate in the program.

Consultation. In Section 1361A (f)(3) of the legislation establishing NFIP it requires States and local communities consult, to the extent practicable, with the owner of the property to determine the appropriate activities. In section 79.7(a) of the Regulations it states, "States and communities shall consult, to the extent practicable, and in accordance with criteria determined by the Director, with owners of severe

repetitive loss properties to select the most appropriate eligible mitigation activity. These consultations shall be initiated in the early stages of project development, and shall continue throughout the process. After FEMA awards the project grant, the subgrantee shall continue to consult with the property owners to determine the specific conditions of the offer."

Voluntary Participation. In section 79.7(b)(1) of the Regulations for NFIP it states, "the offer will clearly state that the property owner's participation in the SRL program is voluntary."

In addition, section 79.5(a)(3) states, "participation in these flood mitigation grant programs is voluntary, and States may elect not to participate in either the SRL or FMA programs in any fiscal year without compromising their eligibility in future years" and section 79.5(b) states that "Participation in the Severe Repetitive Loss and Flood Mitigation Assistance program is voluntary and communities may elect not to apply."

Pursuant to these requirements, the eGrants program guidance requires the local community consult with individuals prior to submitting a sub-application. An individual's participation is voluntary and the individual is advised of the voluntary nature of the programs. Individual property owners cannot apply directly to FEMA themselves. FEMA Mitigation grant programs are voluntary, so no information is required unless an individual property owner is voluntarily requesting assistance through an eligible State or local community.

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

As stated above, FEMA Mitigation grant programs are voluntary so no information is required unless an individual property owner voluntarily requests assistance through an eligible State or local community. FEMA posted a Privacy Statement (Appendix B) and published a SORN (Appendix A) which include the disclosure of routine uses for FEMA, States and local community users of the eGrants web site. States and local communities are required to share the SORN with individuals that are included in an application for FEMA mitigation grants; however, FEMA does not collect consent forms or other documents that validate whether the State has shared the Privacy Statement. Please see the attached SORN for the "NEMIS-MT e-Grants, Mitigation Electronic Grants Management System" for a complete listing of routine uses for this information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The NFIP statute requires consultation with individuals before involving them in the grant process. Additionally, states are expected to inform individuals that participation is completely voluntary. These statutory requirements have been implemented in the eGrants program guidance. FEMA does not have direct contact with the individuals, but provides the notice or disclosure to the State to share with individuals. FEMA has published a Privacy Notice on the eGrants website and has published a formal SORN detailing the limited use of the personally identifiable information collected in eGrants.

The risk exists that States and local communities do not provide individuals with the adequate notice of the potential uses for their information. The SORN and Privacy Statement provide some mitigation, but FEMA is not in a position to monitor the information day to day collecting practices of the States and local communities. However, States and local communities are bound by statutory requirements implemented into the eGrants program guidance by FEMA which mandate no individuals have their information collected without their explicit permission and consultation.

Section 7.0 Individual 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 which allow individuals to gain access to their own information?

For individual property owners whose information has been submitted to FEMA as part of an application, the individual may request in writing a copy of his or her information in the system by contacting FEMA at:

1. The FEMA Regional Office in which they reside and request a copy of their information, in which case the request is referred to the Regional FOIA contact, or
2. "Privacy Act/FOIA request" Federal Emergency Management Agency Office of Chief Counsel (Headquarters), Room 840, 500 C Street, SW, Washington, DC 20472, (202) 646-3051, (202) 646-3958 (tele-fax).

7.2 What are the procedures for correcting erroneous information?

If the individual gains access to their personally identifiable information according to Section 7.1 above and in the process identifies erroneous information, the individual may bring this to the attention of officials of the State or local community, as appropriate, in order to have the information corrected during any point of the application development, review, approval, or award process. Individual property owners may also request in writing a correction to their information in the system by contacting FEMA one of the following two ways:

1. Contact the FEMA Region Office in which they reside and request a copy of their information, or
2. Contact the Privacy Act Officer, FEMA Office of Chief Counsel, Federal Emergency Management Agency (Headquarters), Room 840, 500 C Street, SW, Washington, DC 20472, (202) 646-3949, (202) 646-4536 (tele-fax).

FEMA user rights do not allow FEMA users to amend or revise any information submitted by a State. Where a FEMA user discovers erroneous information, including information about an individual property owner, the system is designed to allow for revisions to the information at any time prior to the grant award and for amendments to the information after the grant award. Mitigation staff at FEMA would

notify the State or the local community who would in turn contact the individual property owner to obtain and verify the correct information, after which the State or local community would enter the correct information in the application and resubmit to FEMA. It is important to note that it is very unlikely that a FEMA user would be able to identify erroneous information about individual property owners. Only the State or local community would know if it has captured such information correctly in the application from the individual property owners.

The Internet-based program gives local community users the opportunity to input new data or use data they have previously entered to develop and manage sub-applications, including applications for activities to mitigate individuals' properties. These updates would be submitted via the Internet-based program to the corresponding State for review, and the State would decide whether or not to include each sub-grant application in their grant application for submittal to FEMA. Once the local community submits the application, including the individual's information, the application cannot be edited, unless the State releases the application back to the local community. This process ensures that only those authorized State and local community users have access to the data, whether that access is for "Create/Edit," "Sign/Submit," and/or "Read-Only" purposes.

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

Individuals work directly with their State or local community and are informed of the procedures for correcting their information by their State or community at the time the information is collected.

7.4 If no redress is provided, are alternatives available?

Redress is provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Access, correction, and redress rights are provided to individuals with information collected under the eGrants system. FEMA, States, and local communities are primarily responsible for ensuring the information is correct and, if not, correcting and providing the information to the individuals upon request. Ample technical measures allow a State to edit information submitted to FEMA.

Section 8.0 Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

Access to the eGrants system (Internet- or Intranet-based programs) and its data is for official purposes only and differs based upon each user's authorized work-related functions. Each user is granted access only to the extent necessary to accomplish his/her official duties. FEMA maintains a unique profile for each user, including the different access rights based on the specific grant program and the parts of the applications (called "queues") within the Intranet-based or Internet-based programs that the user is assigned. Individual property owners do not have access to the information in the system, other than as explained under Section 7.0. The users who are authorized to access the data in the system may be one of the following:

- FEMA Mitigation Division and Grants Management Office (staff, managers, and contractors), who receive grant applications from Applicants/States and review/evaluate or approve/sign, as appropriate;
- FEMA Information Technology Services Division (system administrators and contract developers), who correct any potential errors and trouble-shoot any problems or issues;
- State and Territory emergency management agencies or, similar offices and Federally-recognized Indian Tribes (staff and managers), submit applications to FEMA and are known as Applicants (see Section 1.1); and,
- State agencies, local government agencies and Indian Tribal governments (staff and managers), who create and submit sub-applications and to which sub-grants are awarded, and which are accountable to the Applicant/State for the use of the funds that are provided, and are known as Sub-applicants (see Section 1.1).

Access to data in the system by States and local communities is restricted or limited to registered system users with usernames and passwords and that have been approved to role-based accounts designed to include controls for the principles of least privilege and separation of duties. At the time of registration, new users may be approved for access only to information of the State agency or local community for which they are eligible applicant representatives. Registration is controlled by unique access codes provided by FEMA to the States and to the local communities via the States. Access to new State users may be granted by FEMA after verifying the registered user as an authorized representative of the State. Access for local community agencies may be granted by their respective State agency after verifying the registered user as an authorized representative of that eligible local community agency.

Users may only access the information they entered into the system, but may grant access to that information to other approved users as needed. When a user grants access to information to a second user, the user may specify the level of access the second user may have to that information, but only up to the level of access they have in eGrants itself. For example, if User A grants access to the information in an application to User B, User A may specify whether User B is permitted Read Only, Create/Edit, or Sign/Submit access; however, if User B is only authorized access to eGrants for Read Only, User A may only authorize User B Read Only access to that information.

8.2 Will contractors to DHS have access to the system?

Yes, FEMA information technology staff, contract administrators, and developers who manage the operations and maintenance of the eGrants system have controlled role-based access to the data, in addition to their FEMA usernames and passwords, in order to view and/or trouble-shoot any technical system or data issue that is brought to their attention by the FEMA Mitigation and Grants Management Office system or data leads.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. eGrants uses Role-Based Access Control (RBAC) to control access to both data and functions so that each user is granted the minimum amount of access to the system that is necessary according to his/her official role in the Mitigation grants process. Permissions for access to data and the functions used to manipulate the data have been pre-defined for each FEMA position. Roles have been designed to include controls for the principles of least privilege and separation of duties.

FEMA employee and contractor user roles in the Intranet-based program of the eGrants System are associated with certain parts of the applications (called "queues") when reviewing/evaluating and approving/signing an application. Therefore, depending on the roles assigned to a user, he is only permitted access to queues associated with the roles assigned to him. For example, if a user has been assigned the Regional MT Officer Manager role, he will only have access rights to those applications within his Region, whereas a user who has been assigned the FEMA Headquarters Mitigation role will have access to all applications nationwide. Roles are also defined to allow access only to specific grant programs.

State and local community user access is controlled by the role right(s) users have in the program. A user may be approved for "Create/Edit", "Sign/Submit" or "Read Only" roles. Local community users can only access information for their own agency or organization, and the users' roles determine whether they can Create/Edit application information, Sign/Submit the application, or just simply read the information. State users can read all information submitted by the corresponding sub-applicants/local communities. If the State users have the Create/Edit role, they may also enter or change certain allowable information submitted by the local communities. All other information must be released back to the local communities should revisions be necessary.

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

The eGrants system may be accessed through both the Internet and the FEMA Intranet. The users of the Internet-based program are employees from agencies that apply for grants (States and local communities). The users of the Intranet-based program are FEMA bureaus and offices (employees and contractors of FEMA Mitigation Division, Grants Management Office, and Information Technology Services Division) who review/evaluate and approve applications and are identified by roles within the system, and who develop, administer, and maintain the system. Individuals with personally identifiable information included in applications do not have direct access to the eGrants system (either the Internet- or Intranet-

based programs), but may contact either States, local communities, or employees and contractors of FEMA to obtain or request changes to their information.

Access rights to eGrants are assigned to users who are FEMA employees and contractors, States, and local communities for official purposes only and is accomplished through the use of two database systems called the NEMIS Access Control System (NACS) and the FEMA Access Management System (FAMS). NACS and FAMS are used together by designated FEMA officials to approve people as users in the system and to assign them with role-based access rights.[5] NACS is the system for controlling users' access and rights to the Intranet-based program of the e-Grants system, and FAMS is the system for controlling users' access and rights to the Internet-based program of the e-Grants system.

Certain FEMA employees are authorized in writing by senior level managers to be given rights in NACS and FAMS to request and approve people as users in the system and to assign them to role-based access rights. The authorized employee (Access Requestor) who requests access rights for a user must be different than the authorized employee (Access Approving Official) who approves that user's access rights that have been requested. A user account is established or updated in NACS for each Intranet-based user, or in FAMS for each Internet-based user. Users are only assigned access to through NACS (Intranet for FEMA employees) or FAMS (Internet for States/ Applicants and communities/sub-applicants), but not both.

For FEMA users (Intranet users), Access Requestors and Access Approving Officials determine access rights for users, depending on their program, roles within the system (e.g. cost reviewer, environmental/ historic preservation, grants management specialist,etc.), and location (Headquarters or Regional) and create role-based access accounts for each FEMA user specific to his/her roles. FEMA users receive data as it is submitted by the States via an application for FEMA grants. FEMA users may not modify the information submitted by the State, but the State may make revisions that are subsequently available for FEMA to view.

For State and local community users, a FAMS user account is assigned after specific access rights are requested and approved. In order to request and approve access, FEMA provides a unique access code to each State, determined in advance between the State and the FEMA Regional program office. With this unique access code, authorized employees of the State are able to provide basic personally identifiable information in order to be granted access to the Internet-based program. Once a user is granted access by FEMA, a unique username and password is automatically sent online that will enable the State employee to access eGrants. With respect to local community registration and access approval, FEMA delegates authority down to the State. Both State and local community user access to the information in the Internet-Based program of the eGrants System is for "Create/Edit", "Sign/Submit", and/or "Read-Only". Following these roles, approved users may access applications for FEMA grants, and modify or submit based on their approved roles. Internet-based program accounts for State and local community remain active until FEMA action is taken to remove them.

[5] Note: NACS and FAMS are presently being combined into the Integrated Security and Access Control System (ISAACS).

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The following controls prevent the misuse of data by users (as described under FEMA's "eGrants Risk Assessment Report (May 15, 2004)").

1. Login to the system is based on an assigned username and password that has a pre-set expiration date that is automatically imposed. The username and password will exist for only a limited amount of time, and the user will only have access to the system during the period of time both of these controls exists. If a user's access to the system has expired, he or she will be unable to login to the eGrants system.
2. Based on the username, the system identifies the role assigned to the user and determines the extent of the user's rights and controls access. Users with limited or restricted access will be unable to navigate to all links on the website. Pop-up windows noting "restricted viewing" will appear.
3. The system will not allow a user to bookmark the URL of the eGrants system with the intent of returning to that page at another time without entering the user ID and password. If an attempt is made to use the bookmark to access the eGrants system the user will automatically be redirected to the login page where the user must enter a valid user ID and password in order to gain access to the eGrants system.
4. If an active eGrants browser window is left open with no actions taken within the system, the displayed page will expire after 30 minutes. The user can then re-login using the username and password to access the system.
5. The eGrants software is designed so that access to "Read" or "Edit" certain information complements the role-based rights of the users. The Applicant/State or the sub-applicant/local community must recall, revise, and re-submit the application, according to criteria, procedures and controls designed within the software itself. FEMA employees and contractors who have responsibilities to review and approve application information will see the application in the "Read-Only" format. While they can provide comments and make edits in the eGrants System relative to FEMA's review and approval processes, they cannot alter the application. If any changes or revisions are needed to the application it must be released back to the Applicant/State to make the edits to the application, either in whole or in part. Further information on criteria, procedures, and controls designed in the system software can be found in sections 3.1 and 3.2 of the "*Software Requirements Specification Document (SRS), FEMA Mitigation Program for e-Grants system (External Interface – Grant/Sub-grant), Document Number 101, Date Revised 10/10/2002*".
6. FEMA Enterprise Operations and the Office of Cyber Security are able to monitor system use and determine whether information integrity has been compromised and whether corrective action by the Office of the CIO is necessary. Their procedures are compliant with Title III of the E-Government Act of 2000 (Federal Information Security Management Act).

7. As unauthorized attempts to upload or change information are prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act, FEMA employs software programs that monitor host and network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage. Activity in eGrants can be tracked as the system maintains an audit trail of user information when access is accomplished or any activity performed.

If an unauthorized user is detected, FEMA may revoke access to that user registration. As previously described in Section 8.1, access to data in the system is restricted. At the time of registration, new users may be approved for access only to information for the State and local community for which they are eligible applicant representatives. If unauthorized access is detected, FEMA notifies the State in which the unauthorized access occurred, and revokes access to that user registration.

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

Because unauthorized attempts to upload information or change information are prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act, FEMA employs software programs that monitor host and network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage by users in the system. The system maintains an audit trail of all changes made to any application and the user information associated with those changes.

If an unauthorized user is detected, FEMA may revoke access to that user registration. As previously described in Section 8.1, access to data in the system is restricted. At the time of registration, new users may be approved for access only to information for the State and local community for which they are eligible applicant representatives. If unauthorized access is detected, FEMA notifies the State in which the unauthorized access occurred, and revokes access to that user registration.

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

FEMA, State, and local community staff are trained specifically on how to obtain and/or grant access rights and assign user roles that govern access to information in the system. Training generally includes how to access the system as well as the types of information collected in the system, including information covered under the Privacy Act.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Consistent with the requirements of the Federal Information Security Management Act (FISMA), FEMA is committed to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction in order to provide integrity, confidentiality, and

availability of the information in the eGrants system. Specifically, the eGrants system System Certification and Accreditation was made effective on September 28, 2004.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The eGrants system presents two major issues: protection of the information and user access controls. Each of these risks is mitigated by robust access controls and auditing capabilities within the eGrants system. Access to personally identifiable information is closely guarded. By achieving its Certification and Accreditation eGrants has demonstrated to the Chief Information Officer that its system security has been properly analyzed and contains the appropriate protection measures for the collection of personally identifiable 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 Was the system built from the ground up or purchased and installed?

This system was build from the ground up by FEMA.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

No, FEMA has not evaluated competing technologies on their privacy handling capabilities.

9.3 What design choices were made to enhance privacy?

No changes were made to system architectures, hardware, software or implementation plans as a result of a privacy impact assessment.

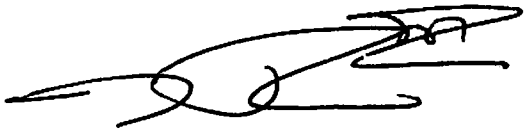
Conclusion

The eGrants system collects personally identifiable information for persons that own property which may be eligible for FEMA mitigation grants. FEMA is authorized to collect this information for the specific use of determining eligibility, and has developed the eGrants system to collect and maintain this information. Individuals must voluntarily request assistance through their State or local community, and therefore do not apply directly to FEMA, nor are they granted direct access to the eGrants system. All information is collected online, and information secured on FEMA servers. This Privacy Impact Assessment demonstrates that FEMA has mitigated potential risks associated with the access, sharing, and retention of personally identifiable information that may be contained in an application.

Responsible Officials

Shabbar Saifee
Federal Emergency Management Agency (FEMA)
Mitigation Division
Risk Reduction Branch
Grants Data Analysis & Tools Section

Approval Signature



Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security