

[Federal Register Volume 69, Number 240 (Wednesday, December 15, 2004)]  
[Notices]  
[Pages 75079-75081]  
From the Federal Register Online via the Government Printing Office  
[<http://www.gpo.gov/>]  
[FR Doc No: 04-27462]

---

DEPARTMENT OF HOMELAND SECURITY

Federal Emergency Management Agency

[DHS-2004-0019]  
RIN 1660-ZA07

National Emergency Management Information System--Mitigation  
Electronic Grants Management System; Privacy Act System of Record

AGENCY: Federal Emergency Management Agency, Emergency Preparedness and  
Response Directorate, Department of Homeland Security.

ACTION: Notice of a new system of records.

---

SUMMARY: Pursuant to the requirements of the Privacy Act of 1974, as amended, the Department of Homeland Security, Emergency Preparedness and Response Directorate, Federal Emergency Management Agency is establishing a new system of records entitled National Emergency Management Information System--Mitigation Electronic Grants Management System. Some (but not all) applications for mitigation grants propose activities that impact properties that are privately owned by individuals (e.g., acquisition of a home that has been repeatedly flooded) and these applications include personally identifiable information about the property owners. Potentially, this personally identifying information may be part of a State's application, and also part of a local community's application as a sub-applicant. Personal information collected in these applications includes the minimum amount necessary to ascertain the eligibility of that property and/or structure (e.g., house or commercial building) under mitigation grant program regulations. See <https://portal.fema.gov/famsVu/dynamic/mitigation.html>.

EFFECTIVE DATE: The addition of a new system of records and routine uses will become effective on January 24, 2005, unless comments are received that result in a contrary determination.

ADDRESSES: You may submit comments, identified by EPA Docket Number: DHS-2004-0019 and/or 1660-ZA07 by one of the following methods:

EPA Federal Partner EDOCKET Web Site: <http://www.epa.gov/feddocket>. Follow instructions for submitting comments on the Web site. DHS has joined the Environmental Protection Electronic Docket System (Partner EDOCKET). DHS and its agencies (excluding the United States Coast Guard (USCG) and Transportation Security Administration (TSA))

will use the EPA Federal Partner EDOCKET system. The USCG and TSA [legacy Department of Transportation (DOT) agencies] will continue to use the DOT Docket Management System until full migration to the electronic rulemaking federal docket management system occurs in 2005.

Federal e-Rulemaking Portal: <http://www.regulations.gov/>.  
Follow the instructions for submitting comments.

Fax: (202) 646-4536.

Mail: Rules Docket Clerk, Federal Emergency Management Agency, Office of General Counsel, Room 840, 500 C Street SW., Washington, DC 20472.

FOR FURTHER INFORMATION CONTACT: Rena Y. Kim, Privacy Act Officer, Federal Emergency Management Agency, Room 840, 500 C Street SW., Washington, DC 20472, (202) 646-3949, (not a toll free call), (telefax) (202) 646-3949, or email [Rena.Kim@dhs.gov](mailto:Rena.Kim@dhs.gov).

SUPPLEMENTARY INFORMATION: 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. 5 U.S.C. 552a. 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 from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Individuals may request their own records that are maintained in a system of records in the possession or under the control of Department of Homeland Security (DHS) by complying with DHS Privacy Act regulations, 6 CFR part 5, subpart B and Federal Emergency Management Agency's (FEMA) Privacy Act regulations, 44 CFR part 6.

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 recordkeeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist the individual to more easily find such files within the Agency.

The Emergency Preparedness and Response Directorate/FEMA is establishing a new system of records pursuant to the Privacy Act of 1974 for the National Emergency Management Information System--Mitigation Electronic Grants Management System (NEMIS-MT eGrants). FEMA intends to collect personal information in applications for its mitigation grant programs through the NEMIS-MT eGrants via the Internet. The FEMA mitigation grant programs are the Flood Mitigation Assistance (FMA) grant program (42 U.S.C. 4104c) and the Pre-Disaster Mitigation (PDM) grant program, (42 U.S.C. 5133). The purpose of FEMA mitigation grant programs is to provide funds to eligible Applicants/States to implement mitigation activities to reduce or eliminate the risk of future damage to life and property from disasters.

Eligible applicants for FEMA mitigation grants are State emergency management agencies or a similar State office that has emergency management responsibility, the District of Columbia, the United States Virgin Islands, the Commonwealth of Puerto Rico, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, and Federally recognized Indian Tribal governments. Eligible Sub-applicants of FEMA mitigation grants are State agencies, local governments, or Indian Tribal governments to which a sub-grant is awarded. Examples of

mitigation activities that impact privately owned properties (and which may include personally identifiable information in a State or local community application) include retrofitting structures, elevation of structures, acquisition and demolition or relocation of structures, minor structural flood control projects, or construction of safe rooms. The personally identifying information

[[Page 75080]]

collected includes an individual's name, home phone number, office phone number, cell phone number, damaged property address, and mailing address of the individual property owner(s), and the individual's status regarding flood insurance, National Flood Insurance Program (NFIP) Policy Number and Insurance Policy Provider for the property proposed to be mitigated with FEMA funds. This notice will make the public aware of routine management and oversight information sharing between FEMA and other Federal agencies, State and local governments, and contractors providing services in support of FEMA mitigation grant programs.

Accordingly, the NEMIS-MT eGrants Privacy Act system of records is added to read as follows:

System Name:

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

System location:

All servers are operated at FEMA, Mount Weather Emergency Operations Center (MWEOC), 19844 Blue Ridge Mountain Road, Bluemont, VA 20135.

Categories of individuals covered by the system:

This system of records notice applies only to individuals identified by name or other individual identifier, such as home address, in the NEMIS-MT eGrants, and includes individuals who are private property owners. These individuals voluntarily request that their State, Territory or local community submit an application for FEMA mitigation grant funds for the purpose of mitigating their property and/or structure (e.g., house or commercial building).

Categories of records in the system:

The categories of records in the system are grant applications. The personally identifying information collected includes an individual's name, home phone number, office phone number, cell phone number, damaged property address, and mailing address of the individual property owner(s), and the individual's status regarding flood insurance, National Flood Insurance Program (NFIP) Policy Number and Insurance Policy Provider for the property proposed to be mitigated with FEMA funds.

Authority for maintenance of the System:

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5133, and the National Flood Insurance Act, 42 U.S.C. 4104c.

Purpose(s) :

The purpose of this system of records is to collect and maintain individually identifiable information in applications for FEMA mitigation grants that are submitted electronically, via the Internet, through the NEMIS-MT eGrants from eligible Applicants/States and Sub-applicants/local communities. The personally identifiable information will be collected and maintained in order for FEMA to ascertain eligibility of the property or structure for FEMA's mitigation grant programs, to verify eligibility of activities for mitigation grants, to identify repetitive loss properties, and to implement measures to reduce future disaster damage.

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), all or a portion of the records or information contained in this system may be disclosed outside FEMA/EP&R/DHS as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

(1) To another Federal agency, State, United States Territory or Tribal government agency charged with administering Federal mitigation or disaster relief programs to prevent a duplication of efforts or a duplication of benefits between FEMA and the other agency. FEMA may disclose information to a State, U.S. Territory, Indian Tribal, or local community agency eligible to apply for mitigation grant programs administered by FEMA.

(2) To contractors, grantees, experts, consultants, students and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records.

(3) To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

(4) 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.

(5) Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law--criminal, civil, or regulatory--the relevant records may be referred to an appropriate Federal, state, territorial, tribal, local, international, or foreign agency law enforcement authority or other appropriate agency charged with investigating or prosecuting such a violation or enforcing or implementing such law.

(6) To the Department of Justice (DOJ) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee, or

(d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation.

(7) To the NARA or other Federal Government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. sections 2904 and 2906.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

All information is stored on secure-access servers operated at a

single site at the FEMA, MWEOC, 19844 Blue Ridge Mountain Road, Bluemont, VA 20135. Backup is provided on a separate server at the same secure facility. MWEOC is only accessible by authorized persons, including FEMA employees and contractors, and entry to the facility is permitted only with a badge issued by the MWEOC.

#### Safeguards:

Safeguards exist in the NEMIS-MT eGrants to prevent the unauthorized access or misuse of data. First, FEMA maintains security safeguards that prevent unauthorized access to the system by assigning each authorized user a unique user profile, username and password based upon his/her official use of the NEMIS-MT eGrants. Each unique profile includes different levels of access rights. For Applicants/States and Sub-applicants/local communities, roles in the system via the Internet are assigned as Read-Only, Create/Edit, or Sign/Submit, and levels of access are assigned by mitigation grant program (i.e., FMA and/or PDM). For FEMA employees and contractors, levels of access via the FEMA Intranet are assigned by mitigation grant program (i.e., FMA and/or PDM) and by Region(s), and roles for FEMA users do not allow FEMA users View information submitted in applications. Passwords expire after a limited time, and users only have access to the system during the period of time that both the assigned username and password are active.

[[Page 75081]]

Access to NEMIS-MT eGrants via the Intranet is assigned to the FEMA employees and contractors for official purposes only through the NEMIS Access Control System (NACS), which controls access to all software available on the FEMA Intranet, and manages roles for FEMA officials accessing the system. Access to NEMIS-MT eGrants via the Internet is assigned to the Applicants/States and Sub-applicants/local communities for official purposes only through the FEMA Access Management System, which performs a similar function to NACS, but for eligible mitigation grant program Applicants/States and Sub-applicants/local communities, and managed roles for these non-FEMA users. The functions of these two databases will be combined into the Integrated Security and Access Control System. While the system is accessed, if an active NEMIS-MT 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. In addition, the system will not allow a user to bookmark the URL of the MT eGrants with the intent of returning to that page at another time without first entering the authorized username and password. Finally, FEMA Enterprise Operations and the Office of Cyber Security are able to monitor system use and determine whether information integrity has been compromised by unauthorized access or use, and whether corrective action by the Office of the Chief Information Officer is necessary. Procedures are compliant with Title III of the E-Government Act of 2000 (Federal Information Security Management Act).

#### Retention and Disposal:

In accordance with U.S. National Archives & Records Administration records retention regulations (GRS 3, 13), records are retained for 6 years and 3 months. Unsuccessful grant application files will be stored in NEMIS-MT eGrants for 3 years from the date of denial, and then deleted. Successful grant application files will be stored in the NEMIS-MT eGrants for 6 years and 3 months from the date of closeout

(where closeout is the date FEMA closes the grant in its financial system) and then deleted. Computerized records are stored in a database server in a secured file server room. Hard copy records are maintained for 6 years and 3 months years, at which time they are retired to the Federal Records Center. The same retention schedule that applies to paper records will be followed. This is consistent with the records retention schedule that has been developed for this system.

System Manager(s) and Address:

Patricia Bowman, Program Manager, IT-SE-CS, 500 C Street SW.,  
Washington DC 20472, Pat.[Bowman@dhs.gov](mailto:Pat.Bowman@dhs.gov), (202) 646-2661.

Notification Procedures:

Address inquiries to the System Manager named above.

Record Access Procedures:

A request for access to records in this system may be made by writing to the System Manager, identified above, in conformance with 6 CFR part 5, subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS and FEMA's Privacy Act regulations at 44 CFR part 6.

Contesting Record Procedures:

Same as Notification procedures above. A request for access to records in this system may be made by writing to the System Manager, identified above, in conformance with 6 CFR part 5, subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS and FEMA's Privacy Act regulations at 44 CFR part 6.

Records Source Categories:

Information in this system of records is obtained from State/Territory, local government, or Indian Tribal government via the Internet to FEMA. While individuals are not eligible Applicants/States or Sub-applicants/local communities, and cannot apply directly to FEMA for assistance, some (but not all) applications for FEMA mitigation grants propose activities that impact properties that are privately owned by individuals (e.g., acquisition of a home that has been repeatedly flooded) and these applications include personal information about the property owners. These individuals voluntarily request that their State, Territory, or local community submit an application for FEMA mitigation grant funds for the purpose of mitigating their property and/or structure (e.g., house or commercial building).

Exemptions Claimed for the System:

None.

Dated: December 10, 2004.

David A. Trissell,  
Associate General Counsel, Emergency Preparedness and Response,  
Department of Homeland Security.

[FR Doc. 04-27462 Filed 12-14-04; 8:45 am]

BILLING CODE 9110-41-P