

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

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

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

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

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

## II. Comments

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

## III. Electronic Access

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

Dated: July 31, 2009.

**Jeffrey Shuren,**

*Associate Commissioner for Policy and Planning.*

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

**BILLING CODE 4160-01-S**

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

### National Institutes of Health

#### National Institute of Environmental Health Sciences; Notice of Closed Meeting

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

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

*Name of Committee:* Environmental Health Sciences Review Committee.

*Date:* August 25-26, 2009.

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

*Agenda:* To review and evaluate grant applications.

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

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

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

Dated: August 3, 2009.

**Jennifer Spaeth,**

*Director, Office of Federal Advisory Committee Policy.*

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

**BILLING CODE 4140-01-P**

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

[Docket Number DHS-2008-0159]

#### Privacy Act of 1974; DHS/FEMA-004 Grant Management Information Files System of Records

**AGENCY:** Privacy Office; DHS.

**ACTION:** Notice of Privacy Act system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of Homeland Security is giving notice that it proposes to consolidate into one new system its inventory of record systems entitled, Federal Emergency Management Agency Grant Management Information Files. This system will enable the Department of Homeland Security to better administer the Federal Emergency Management Agency Disaster Recovery Assistance Program. Many Federal Emergency Management Agency grant programs collect a minimum amount of contact and grant project proposal information. The information contained in the Federal Emergency Management Agency's Grant Management Information Files is collected in order to determine awards for both disaster and non disaster grants and for the issuance of awarded funds.

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

**ADDRESSES:** You may submit comments, identified by DHS–2008–0159 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information, such as email address, provided.
- *Docket:* For access to the docket to read background documents or comments received go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact: Alisa Turner (202–646–3102), Branch Chief, Disclosure Office, Federal Emergency Management Agency, Washington, DC 20472. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

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

investments, and the demonstrated need for the grant funds.

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

Consistent with DHS’s information sharing mission, information stored in the Grants Management Information Files may be shared with other DHS components, as well as appropriate federal, state, local, tribal, foreign, or international government agencies. This sharing will take place only after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

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

**II. Privacy Act**

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a “system of records.” A “system of records” is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the FEMA Grants Management Information Files system of records.

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

**SYSTEM OF RECORDS DHS/FEMA–004**

**SYSTEM NAME:**

DHS/FEMA–004 Grant Management Information Files.

**SECURITY CLASSIFICATION:**

Unclassified and sensitive.

**SYSTEM LOCATION:**

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

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

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

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Categories of records in this system include:

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

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

Legal authority includes, but is not limited to:

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

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

**PURPOSE(S):**

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

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when:

1. DHS or any component thereof;
2. Any employee of DHS in his/her official capacity;
3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed

compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

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

I. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:****STORAGE:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

**RETRIEVABILITY:**

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

**SAFEGUARDS:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The system maintains a real-time auditing function of individuals who access the system. Additional safeguards may vary by component and program.

**RETENTION AND DISPOSAL:**

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

**SYSTEM MANAGER AND ADDRESS:**

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

**NOTIFICATION PROCEDURE:**

Individuals or entities seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the

component's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., STOP-0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, <http://www.dhs.gov> or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

**RECORD ACCESS PROCEDURES:**

See "Notification procedure" above.

**CONTESTING RECORD PROCEDURES:**

See "Notification procedure" above.

**RECORD SOURCE CATEGORIES:**

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

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

Dated: July 31, 2009.

**Mary Ellen Callahan,**

*Chief Privacy Officer, Department of  
Homeland Security.*

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

**BILLING CODE 9110-17-P**

**DEPARTMENT OF THE INTERIOR****Bureau of Indian Affairs****Class III Gaming; Tribal Revenue Allocation Plans; Gaming on Trust Lands**

**AGENCY:** Bureau of Indian Affairs, Interior.

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

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

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

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

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

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

**SUPPLEMENTARY INFORMATION:****I. Abstract**

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