Privacy Impact Assessment
for the

Grant Management Programs

FEMA/PIA-013

February 19, 2015

Contact Point
Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
(202) 212-5100

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) administers and manages grants to enhance the level of preparedness of its customers and stakeholders and the public's ability to prevent, protect, mitigate against, and respond to and recover from all hazards. FEMA determines awards for both disaster and non-disaster grants and manages the grant lifecycle for all grantees, as well as internal and external partners, and ensures critical and measurable results. FEMA updated and republished this Privacy Impact Assessment (PIA) because FEMA collects personally identifiable information (PII) information from grant applicants as part of the grant application process.[1]

Overview

The primary mission of the Federal Emergency Management Agency (FEMA) is to reduce the loss of life and property and protect the nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters. This mission is accomplished by leading and supporting the nation in a risk-based, comprehensive, emergency management system of preparedness, protection, response, recovery, and mitigation. To better prepare America for these hazards, one of FEMA's objectives is to develop and implement national assistance programs. These programs enhance the capacity of state, local, tribal, and territorial governments to respond to incidents through coordinated training, equipment acquisition, technical assistance, and support for federal, state, local, tribal, and territorial exercises. Another one of FEMA's objectives is to provide assistance to state, local, tribal, and territorial governments, and certain types of non-profit organizations to assist communities in their effort to quickly respond to and recover from major disasters or emergencies declared by the President. FEMA provides supplemental federal disaster grant assistance through these programs for debris removal, emergency protective measures, and the repair, replacement, or restoration of disaster-damaged, publicly owned facilities and the facilities of certain non-profit organizations.

FEMA fulfills these objectives through a series of grant programs responsive to the specific needs of state, local, tribal, and territorial governments. FEMA's grant programs implement objectives addressed in the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended;[2] the post-Katrina Emergency Management Reform Act (PKEMPRA) of 2006;[3] and Homeland Security Presidential Directives (HSPD).

---

[1] This updated/reissued PIA replaces DHS/FEMA/PIA-013 Grant Management Programs, published on July 14, 2009.

[2] Pub. L. 93-288, as amended, 42 U.S.C. § 5121 et seq., *available at* http://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg4689.pdf.

[3] Pub. L. 109-295, 6 U.S.C. § 762, *available at,* http://www.gpo.gov/fdsys/pkg/PLAW-109publ295/pdf/PLAW-109publ295.pdf.

FEMA's grant programs provide funding to enhance the capacity of state, local, tribal, and territorial jurisdictions for preparedness and recovery. 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, the U.S. Virgin Islands, certain types of non-profit organizations, and some private entities.

This PIA covers both non-disaster grants and disaster grants. These grants, while both administered by FEMA, differ significantly. Disaster grants are those awards for public assistance, hazard mitigation, and other grants issued pursuant to a Presidentially-declared disaster or emergency. Non-disaster grants are not associated with a Presidential declaration and include homeland security, emergency management, fire fighter assistance, pre-disaster mitigation, and related grants. This PIA does not cover recovery programs directed at individuals such as Individual Assistance or hazard mitigation grant programs, each of which is covered by a respective PIA.[4]

Typical Transactions for the Grant Application Process

Non-Disaster Grants

Non-disaster grants are directed at state, local, tribal, and territorial governments, and certain types of private, nonprofit organizations to enhance their preparedness capacity to prevent, respond to, and recover from a weapon of mass destruction terrorism incident involving chemical, biological, radiological, nuclear, explosive devices, and cyber-attacks. These applicants are required to provide information to determine the eligibility of an activity justifying grant funding.

A typical transaction requires grant applicants to first register to use the General Services Administration's (GSA) System for Award Management (SAM), as the central government-wide menu of grant options. SAM is the Federal Government's procurement and award support system.[5] After grant applicants register on Sam.gov, they can search or apply for FEMA-funded grant opportunities on the Department of Health and Human Services' (HHS) Grants.gov grants management system,[6] which FEMA uses as a service provider to in-take grant applications.

---

[4] DHS/FEMA/PIA-012(a) Disaster Assistance Improvement Plan (DAIP), *available at* http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_fema_daip_20121116.pdf; and DHS/FEMA/PIA-025 Hazard Mitigation Grant Program (HMGP) System, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-fema-hmgp.pdf.

[5] For more information about GSA SAM, please visit the website, *available at* http://www.sam.gov and the SAM PIA, *available at* http://www.gsa.gov/portal/getMediaData?mediaId=174407. Further information regarding the systems of record notice for SAM can be found in the GSA/GOVT-09 System of Award Management System of Records, 78 FR 11648 (February 19, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03743.pdf.

[6] For more information about the HHS Grants Management System please visit the grants.gov website, *available at* http://www.grants.gov and the 06.3 HHS PIA for Grants.gov System, *available at* http://www.hhs.gov/pia/os_pia_summaries_fy12_q2.pdf. A SORN is not required for Grants.gov under the Privacy

Grants.gov transfers applicant information to one of FEMA's web-based grant management systems after the applicant provides his or her information to support the grant application. Applicants can also monitor the status of their application through the one of the web-based grant management systems

FEMA requests information from applicants during the application process and during the life-cycle of an awarded contract to ensure that requirements of federal statutes, regulations, and policies are met. This usually includes contact information and the organization's bank account numbers, routing numbers, and information about the activity or activities proposed to be completed under the requested grant. FEMA also collects financial information as part of the grant process to facilitate electronic funds transfer from FEMA's Web Integrated Financial Management Information System (Web-IFMIS)[7] to the grantee after the final award determination. A FEMA grants specialist then retrieves and reviews the application and makes a determination on grant eligibility and award.

Disaster Grants

FEMA also assists state, local, tribal, and territorial governments and certain types of private, nonprofit organizations with facilitating response and recovery from the devastating effects of disasters by providing technical assistance and financial disaster-related grants and loans. Disaster grants are financial or direct assistance for debris removal; emergency protective measures; the repair, replacement, or restoration of disaster-damaged, publicly-owned facilities; or other recovery activities. FEMA disaster grants (including the Public Assistance program) provide the most significant amount of federal funding and are the largest grant programs in DHS.

The disaster grant application process typically begins after a Presidentially-declared disaster; however, FEMA may collect information from grant applicants prior to the disaster declaration. Unlike with its non-disaster grants, FEMA does not use the Grants.gov portal to collect applications for its disaster grants. FEMA uses its own web-based disaster grants management and financial system to manage disaster grants throughout the entire grant life cycle. The remainder of the application process for disaster grants is the same as the non-disaster grants application process.

Appeals and Arbitrations

At times a grant applicant or grantee may disagree with FEMA regarding a determination related to their request for public assistance (PA). Such disagreements may include whether an applicant, facility, item of work, or project is eligible for PA; whether approved costs are

---

Act of 1974.

[7] For more information about Web-IFMIS please see the DHS/FEMA/PIA-020(a) Web Integrated Financial Management Information System (Web-IFMIS), *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-fema-web-ifmis-20130816.pdf.

sufficient to complete the work; whether a requested time extension was properly denied; whether a portion of the cost claimed for the work is eligible; or whether the approved scope of work is correct. In such circumstances, the applicant may appeal FEMA's determination as described in 44 CFR § 206.206, Emergency Management and Assistance Appeals.[8] FEMA authorizes an appeal process for applicants that dispute a FEMA determination for PA.

Arbitration for Hurricanes Katrina and Rita: The American Recovery and Reinvestment Act of 2009[9]

The American Recovery and Reinvestment Act of 2009 (ARRA) requires the President to establish an arbitration panel under FEMA's Public Assistance program to expedite recovery efforts from Hurricanes Katrina and Rita within the Gulf Coast region. The ARRA further requires the arbitration panel to have sufficient authority regarding the award or denial of disputed PA applications for covered hurricane damage under sections 403, 406, or 407 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act.[10]

Arbitration for Hurricane Sandy: Section 1105 of the Sandy Recovery Improvement Act of 2013[11]

Section 1105 of the Sandy Recovery Improvement Act of 2013 directs FEMA to establish a nationwide Dispute Resolution Pilot Program (DRPP) in order to facilitate an efficient recovery from major disasters, including arbitration by an independent review panel, to resolve disputes relating to PA projects.[12]

Privacy Risks and Mitigations

The primary privacy risks associated with the grant management application process are that FEMA may collect more information from its grant applicants than is necessary, and that inaccurate information may impact the grant eligibility of an applicant. These risks are mitigated because FEMA requires scope-specific information collection in accordance with FEMA policies and current operating procedures so that grant programs only collect information relevant and necessary to determine award eligibility. FEMA grant specialists verify information submitted in grant applications and systems. Additionally, FEMA affords grant applicants the opportunity to review and correct any erroneous information through providing access to the IT systems supporting the grants process.

---

[8] 44 CFR § 206.206, *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title44-vol1/xml/CFR-2011-title44-vol1-sec206-206.xml.
[9] Pub. L. 111-5, 26 U.S.C. § 1 *et seq.*, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/html/PLAW-111publ5.htm.
[10] Pub. L. 93-288, as amended, 42 U.S.C. § 5121, et seq. (*available at* http://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg4689.pdf); implementing regulation, *available at* 44 C.F.R. § 206.209.
[11] Pub. L. 113-2, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-113publ2/pdf/PLAW-113publ2.pdf.
[12] DRPP eligibility criteria, *available at* 44 C.F.R. § 206.210.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

- Department of Homeland Security Appropriations Act, 2014;[13]
- Sandy Recovery Improvement Act of 2013;[14]
- American Recovery and Reinvestment Act of 2009;[15]
- Section 635 of the Post-Katrina Emergency Management Reform Act of 2006;[16]
- Title III of Division D of the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act;[17]
- Title III of Division E of the Consolidated Appropriations Act, 2008;[18]
- Section 1406, Title XIV of the Implementing Recommendations of the 9/11 Commission Act of 2007;[19]
- Section 1513, Title XV of the Implementing Recommendations of the 9/11 Commission Act of 2007;[20]
- Section 1532(a), Title XV of the Implementing Recommendations of the 9/11 Commission Act of 2007;[21]
- Section 614 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act,[22] as amended by Section 202, Title II of the Implementing Recommendations of the 9/11 Commission Act of 2007;[23]
- Section 1809 of the Homeland Security Act of 2002,[24] as amended by Section 301(a), Title III of the Implementing Recommendations of the 9/11 Commission

[13] Department of Homeland Security Appropriations Act, 2014, Pub. L. 113-76, *available at* https://www.congress.gov/bill/113th-congress/house-bill/2217.
[14] Pub.L. 113-2, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-113publ2/pdf/PLAW-113publ2.pdf.
[15] Pub. L. 111-5; 26 U.S.C. § 1 *et seq.*, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/html/PLAW-111publ5.htm.
[16] Pub. L. 109-295, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-109publ295/pdf/PLAW-109publ295.pdf.
[17] Pub. L. 110-329, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ329/pdf/PLAW-110publ329.pdf.
[18] Pub.L. 110-161, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ161/pdf/PLAW-110publ161.pdf.
[19] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[20] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[21] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[22] Pub. L. 93-288, as amended, 42 U.S.C. § 5196c, et seq., *available at* http://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg4689.pdf.
[23] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[24] Pub. L. 107-296, 6 U.S.C. § 571 et seq., *available at* http://www.dhs.gov/homeland-security-act-2002).

Act of 2007;[25]

- Section 2003 of the Homeland Security Act of 2002, as amended;[26]
- Section 2003(a) of the Homeland Security Act of 2002,[27] as amended by Section 101, Title I of the Implementing Recommendations of the 9/11 Commission Act of 2007;[28]
- Section 2004 of the Homeland Security Act of 2002,[29] as amended by Section 101, Title I of the Implementing Recommendations of the 9/11 Commission Act of 2007;[30]
- Section 2004(a) of the Homeland Security Act of 2002,[31] as amended by Section 101, Title I of the Implementing Recommendations of the 9/11 Commission Act of 2007;[32]
- Section 2005 of the Homeland Security Act of 2002,[33] as amended by Section 101, Title I of the Implementing Recommendations of the 9/11 Commission Act of 2007;[34]
- Section 102 of the Maritime Transportation Security Act of 2002, as amended;[35]
- Federal Financial Assistance Management Improvement Act of 1999;[36]
- Robert T. Stafford Disaster Relief and Emergency Assistance Act;[37]
- Sections 203, 403, 404, 406, 407, and 417 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended;[38] and

---

[25] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[26] Pub. L. 107-296, 6 U.S.C. § 604, *available at* http://www.dhs.gov/homeland-security-act-2002.
[27] Pub. L. 107-296, 6 U.S.C. § 604(a), *available at* http://www.dhs.gov/homeland-security-act-2002.
[28] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[29] Pub. L. 107-296, 6 U.S.C. § 605 et seq., *available at* http://www.dhs.gov/homeland-security-act-2002.
[30] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[31] Pub. L. 107-296, 6 U.S.C. § 101 et seq., *available at* http://www.dhs.gov/homeland-security-act-2002.
[32] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[33] Pub. L. 107-296, 6 U.S.C. § 606 et seq., *available at* http://www.dhs.gov/homeland-security-act-2002.
[34] Pub. L. 110-053, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf.
[35] Pub. L. 107-295, 46 U.S.C. § 70107, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-107publ295/pdf/PLAW-107publ295.pdf.
[36] Pub. L. 106-107, 31 U.S.C. § 6101, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-106publ107/pdf/PLAW-106publ107.pdf.
[37] Pub. L. 93-288, as amended, 42 U.S.C. § 5121 et seq., *available at* http://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg4689.pdf).
[38] Pub. L. 93-288, as amended, 42 U.S.C. §§ 5133, 5170a, 5170b, 5170c, 5173, and 5184; and 42 U.S.C. §§ 4030, 4102a, and 4104c, *available at* http://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg4689.pdf.

- National Historic Preservation Act of 1966, as amended, Pub.L. 89- 665, § 102, 16 U.S.C. § 470.[39]

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following SORNs apply to grant management programs: DHS/FEMA-004 Grant Management Information Files System of Records,[40] which covers non-disaster grant information; DHS/FEMA-009 Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs System of Records,[41] which covers disaster-related grants and loans; and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) System of Records,[42] which covers the records related to the applicants' access to the corresponding IT systems supporting FEMA's disaster and non-disaster grant programs.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. Systems supporting grant management programs are covered by this PIA and are in compliance with the Federal Information Security Management Act (FISMA) of 2002.[43] These systems are listed in Appendix B.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, the records retention schedule for grant management systems and programs covered by this PIA have been approved by the NARA under General Records Schedule (GRS) 3, Items 13 and 14; N1-311-95-001, Items 1, 2, and 3; N1-311-01-008, Item 1; and N1-311-04-001, Item 1.

---

[39] Pub. L. 89- 665, § 102, 16 U.S.C. § 470, *available at*, http://www.gpo.gov/fdsys/pkg/USCODE-2011-title16/pdf/USCODE-2011-title16-chap1A-subchapII-sec470.pdf.
[40] DHS/FEMA-004 Grant Management Information Files System of Records, 74 FR 39705 (August 7, 2009), *available at* http://www.gpo.gov/fdsys/pkg/FR-2009-08-07/html/E9-18931.htm.
[41] DHS/FEMA-009 Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs System of Records, 79 FR 16015 (March 24, 2014), *available at* https://www.federalregister.gov/articles/2014/03/24/2014-06361/privacy-act-of-1974-department-of-homeland-security-federal-emergency-management-agency-009-hazard.
[42] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.
[43] Pub. L. 107-347, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information FEMA collects for its grant programs is covered by PRA and collected through Information Collection Requests (ICRs) as follows:

Non-Disaster ICRs:

- *Emergency Preparedness and Response Directorate Grants Administration Forms* (Office of Management and Budget (OMB) 1660-0025);
- *Assistance to Firefighters Grant Program-Grant Application Supplemental Information* (OMB 1660-0054);
- *Fire Management Assistance Grant Program (*OMB 1660-0058*);*
- *National Urban Search and Rescue Grant* (OMB 1660-0073);
- *Urban Areas Security Initiative (UASI) Non Profit Security Grant Program (NSGP)* (OMB 1660-0110);
- *Transit Security Grant Program (TSGP)* (OMB 1660-0112);
- *Tribal Homeland Security Grant Program (THSGP)* (OMB 1660-0113);
- *Port Security Grant Program (PSGP)* (OMB 1660-0114);
- *FEMA's Grants Reporting Tool (GRT)* (OMB 1660-0117);
- *FEMA Homeland Security Grant Program (HSGP) and Operation Stonegarden (OPSG) Grant Program* (OMB 1660-0119);
- *Regional Catastrophic Preparedness Grant Program (RCPGP)* (OMB 1660-0123);
- *Homeland Security Grant Program (HSGP)* (OMB 1660-0125); and
- *Emergency Management Performance Grant Program* (OMB 1660-0126).

Disaster Related ICRs:

- *Public Assistance Progress Report and Program Forms* (OMB 1660-0017);
- *Application for Community Disaster Loan Cancellation* (OMB 1660-0082)*;* and
- *Community Disaster Loan Program* (OMB 1660-0083).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Information Submitted by Organization Points of Contact (POC) when applying for non-disaster grants:

- Name of Organization's Designated POC;
- POC Title;
- POC's office mailing address;
- POC's office phone number;
- POC's office cellphone number;
- POC's office fax number;
- POC's work e-mail address;
- Organization Name;
- Organization's Federal Employer Identification Number (EIN);
- Organization's Dun & Bradstreet (D&B) Data Universal Numbering System (DUNS) Number;
- Organization's Bank Routing Number; and
- Organization's Bank Account Number.

Information Submitted by Organization POCs when applying for disaster grants:

Records collected from Organizations:

- Name of Organization's Designated POC full name;
- POC Title;
- POC's office mailing address;
- POC's office phone number;
- POC's office cell number;
- POC's office fax number;
- POC's email address;

- Organization Name;
- Organization's Federal EIN;
- Organization's D&B DUNS Number;
- Organization's State Tax Number;
- Organization's Bank Routing Number;
- Organization's Bank Account Number;
- Organization's activity or activities proposed under requested grant; and
- Urban Area Affiliation (if applicable).

IT System Specific Security Information Collected from POCs:

- Role Assignment and User Permissions;
- Unique username;
- Password; and,
  - Security Question, which is one of the following:
    - 1. What is your first pet's name?
    - 2. What is your father's middle name?
    - 3. What is your high school mascot?
    - 4. Who is your childhood best friend?

2.2 What are the sources of the information and how is the information collected for the project?

FEMA collects information from officials and representatives (POCs) of states, local governments, territories, and tribal entities; port authorities; transit agencies; non-profit organizations; inter-city passenger rail systems; and (in rare instances) private companies.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes, pursuant to the Office of Management and Budget (OMB) policy on the Use of a Universal Identifier by Grant Applicants, DHS/FEMA-related grant programs and IT systems require and maintain the DUNS number for grant applicants. FEMA uses the DUNS number for tracking purposes and to validate address and POC information for grantees and sub-grantees.

2.4 Discuss how accuracy of the data is ensured.

Grant specialists verify information about the grantee including the name of the POC for the application, work address, work phone number, and work email address. All grant application information is reviewed for accuracy throughout the lifecycle of the grant application by comparing information regularly submitted by grantees with programmatic and financial reports generated and reviewed by FEMA staff on a quarterly basis. POCs may also directly input the data into FEMA grant supporting IT systems and have the opportunity to review grant application information for accuracy at any point in the grant lifecycle.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that more information is collected from grant applicants than is necessary.

Mitigation: This risk is mitigated because FEMA is required to follow specific guidelines regarding the scope of information collected. Information required from grant applications collected is in accordance with FEMA policies and standard operating procedures. FEMA grant programs only collect information that is necessary to assess grant applications to determine award eligibility.

Privacy Risk: There is a risk that inaccurate information may impact the grant eligibility of an applicant.

Mitigation: This risk is mitigated because grant applicants are able to review their applications prior to submission. Additionally, grant specialists check information submitted by eligible grantees for accuracy and verify information about the grant applicant or grantee. The grant applicant is able to correct identified information before final submission. Grant applicants may contact system administrators for the various grant management systems to request correction of information they have submitted at any stage of the application process. Grant applicants are provided notice of information correction procedures at the initial stage of the application process.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

FEMA may collect information for its non-disaster and disaster grants through paper forms, web-based portals, and IT systems. FEMA collects, reviews, and evaluates grant applicants' supporting information to determine grant eligibility, facilitate communication through the grant lifecycle, and facilitate the award of grant funds. FEMA may share the grant

applicant and grantee information with other agencies to determine if investments meet grant requirements or fall short of eligibility requirements as described in the PIA and SORN. Additionally, FEMA uses this information to generate reports summarizing grant activity. These reports are used to assist in the management and reporting of grant programs including: overall grant management; program- specific progress; functions and monitoring; financial management; management of grantee and sub-grantee (if available); and system administration. Lastly, FEMA collects IT system-specific security information data from grant applicant POCs to access various grant application systems.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information collected will be used for unauthorized purposes that are inconsistent with the original purpose of collection.

Mitigation: This risk is mitigated because grant specialists, system users, and system administrators of the various grant systems are required to protect and use data in accordance with the policies, standards, and regulations specified for each system. FEMA limits its collection and use of information to only what is necessary to determine grant eligibility and facilitate awards. Additionally, grant management programs audit collected information to ensure that data is used for authorized purposes consistent with the original purpose of collection.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This PIA and the SORNs listed in 1.2 serve as notice for information collection. FEMA also provides grant applicants a notice as required by the Privacy Act, 5 U.S.C. § 552a(e)(3). The Privacy Act notice is provided in both paper and electronic versions of the grant application. The notice states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals choose to submit information to FEMA for their organization's grant application to be considered. The organizations can choose not to submit the information, but failure to do so prevents FEMA from considering their grant application. Individuals are notified of the uses of their information prior to collection. Applicants give consent to the uses of their information by providing information on the grant application. FEMA does not use the information outside of the uses or scope outlined in this PIA, the applicable SORNs, and the notice provided on the relevant applications or systems. The PIA, SORNs, and Privacy Act notices will be updated if FEMA anticipates a need for a new use for the information.

4.3 Privacy Impact Analysis: Related to Notice

FEMA provides notice to all individuals in the form of a Privacy Act notice prior to information collection on online applications/systems or paper forms. Notice is also provided after applicants log in to the various web-based systems. Therefore, FEMA has provided clear notice to individuals consistent with the Privacy Act to help address the privacy risk related to notice.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Grant application information is retained for audit, oversight operations, and appeal purposes.

- FEMA destroys grant administrative records and hard copies of unsuccessful grant applications files after two years in accordance with Government Records Schedule (GRS) 3, Item 14.

- FEMA stores electronically received and processed copies of unsuccessful grant application files for three years from the date of denial and then deleted in accordance with GRS 3, Item 13.

- FEMA maintains grant project records 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, in accordance with National Archives and Records Administration (NARA) Authority N1-311-95-001, Item 1.

- FEMA retires grant final reports to the Federal Records Center (FRC) three years after cutoff and transfers them to NARA 20 years after cutoff in accordance with NARA Authority N1-311-95-001, Item 3.

- FEMA stores all other grant records for six years and three months from the date of closeout (when closeout is the date FEMA closes the grant in its financial system) and final audit and appeals are resolved and then deleted in accordance with NARA Authority N1-311-95-001, Item 2; N1-311-01-008, Item 1; and N1-311-04-001, Item 1.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is risk that FEMA will retain information longer than necessary.

Mitigation: FEMA only retains the information in accordance with the established retention schedules above. System Administrators for each of the grant management systems and grant management specialists are responsible for paper applications and for deleting or archiving information in accordance with the retention schedules. An automated annual audit process exists for grant management systems.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

FEMA does not routinely share information outside of DHS as part of normal agency operations; however, information may be shared consistent with routine uses as outlined in the DHS/FEMA-004 Grant Management Information Files SORN; the DHS/FEMA-009 Hazard

Mitigation Disaster Public Assistance and Disaster Loan Programs SORN; and the DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORN.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

As per 6.1 above, FEMA does not routinely share grant application information outside of DHS.

6.3 Does the project place limitations on re-dissemination?

Yes; FEMA places restrictions on re-disseminating outside of the sharing outlined in the SORNs mentioned in section 1.2 of this PIA. FEMA includes a letter to an external organization such as an educational institution or executes an MOU and access agreement with the external agency for all other external sharing of information. These documents indicate that FEMA's records are being transferred for use pursuant to the applicable routine uses and that further disclosure of the records is not permissible.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Requests for records from grant programs or systems are made to the FEMA Disclosure Office, which maintains the accounting of what records were disclosed and to whom as identified in the SORNs listed in 1.2.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be erroneously disclosed outside of DHS.

Mitigation: FEMA mitigates the risk of unauthorized disclosure of grant applicant information because external sharing is limited to requests in writing, pursuant to the routine uses in the respective SORNs and only for the minimum amount of data required to achieve a documented business purpose is shared with external organizations. Robust technical, management, and operational controls are implemented and sharing protocols are in place to confirm access to grant management systems. These access procedures limit access to individuals with a valid "need-to-know," which is also the case for paper applications. Additionally, grant management programs audit disclosures of grant applicant information.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Grant applicants can correct their information by logging into the web-based grant management systems. Additionally, applicants can contact the grant program office or project that initially collected the information or systems administrators for the various grant management systems. Grant applicants may consult the SORNs for additional information regarding how to access their information via Privacy Act or Freedom of Information Act (FOIA) request submitted to the FEMA Disclosure Office. Such requests should be sent to: FEMA Disclosure Officer, Records Management Division, 500 C Street, SW, Washington, D.C. 20472.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

See Section 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

The organization's grant POCs providing the application information to FEMA accesses the same electronic systems used in the application process to correct erroneous information. Additionally, the POCs are notified of the procedures for correcting their information through this PIA as well as through the SORNs listed in Section 1.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that the grant applicant POCs are not able to correct erroneous grant application information.

Mitigation: FEMA mitigates this risk by allowing grant applicants to correct their information by themselves by logging into the web-based system. Grant applicants can correct their information by contacting the grant program office, the project that initially collects the information, or systems administrators for the various grant management systems. Additionally, FEMA manages this risk by informing grant applicants of procedures for correcting their policy information through this PIA and the SORNs listed in Section 1.2.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

FEMA ensures the practices stated in this PIA by leveraging standard operating procedures (SOP), orientation and training, policies, rules of behavior, and biennial user account auditing. Grant management systems use a separation of access capabilities based on process roles. FEMA ensures access to grant applicant information is both restricted and controlled. Grant management systems include the automatic revocation of access upon expiration of privileges. In addition, FEMA audit policy and procedures are written to ensure the grant management systems develop, disseminate, and review/update a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in addition to formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. Audit trail data is reviewed at a minimum of every three days.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

FEMA employees and contractors are required to complete annual privacy and security training. Access to FEMA networks and facilities is denied for FEMA employees who do not complete the required annual training until mandatory training requirements are fulfilled.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Authorized FEMA OCSO personnel or contractors who handle the operations and maintenance of the grant management systems have position-specific access to the system to support the primary system function and troubleshoot technical system issues encountered on a day-to-day basis. All assigned FEMA employees and contractor staff receive appropriate privacy and security training and have any necessary background investigations or security clearances for access to sensitive, private, or classified information. Robust SOPs and system user manuals describe user roles, responsibilities, and access privileges.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

FEMA's process for reviewing and approving MOUs and Information Sharing Agreements involve FEMA's IT Security Branch, FEMA Privacy Officer, and the Office of

Chief Counsel, as well as the appropriate authorities from the other agency or organization to the agreement. FEMA reviews these agreements on an annual basis and reviews appropriate security documents for any newly identified risks. FEMA mitigates any newly identified risks between the partnering agencies in accordance with applicable laws.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
U.S. Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Appendix A: IT SYSTEMS SUPPORTING GRANT MANAGEMENT PROGRAMS

1. Assistance to Firefighters Grants (AFG)
2. Non Disaster (ND) Grants
3. Grants Reporting Tool (GRT)
4. Emergency Management Mission Integrated Environment (EMMIE)
5. National Emergency Management Information System (NEMIS) – Public Assistance (PA)