Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 1 of 7

PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 2 of 7

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Community Disaster Loan (1660-0083)**		
Component:	Federal Emergency Management Agency (FEMA)	**Office or Program:**	Office of Response and Recovery (ORR)- Public Assistance (PA) Division
Xacta FISMA Name (if applicable):	**N/A**	**Xacta FISMA Number (if applicable):**	**N/A**
Type of Project or Program:	**Form or other Information Collection**	**Project or program status:**	**Existing**
Date first developed:	**January 1, 1974**	**Pilot launch date:**	**N/A**
Date of last PTA update	**May 9, 2012**	**Pilot end date:**	**N/A**
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	**N/A**

PROJECT OR PROGRAM MANAGER

Name:	**Martha Polanco**		
Office:	**Public Assistance Division**	**Title:**	Assistant Program Manager
Phone:	**202.701.4023**	**Email:**	Martha.Polanco.2@fema.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**N/A**		
Phone:	**N/A**	**Email:**	N/A

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 3 of 7

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Renewal PTA	

The Office of Response and Recovery, Public Assistance Division's Community Disaster Loan (CDL) Program provides operational funding (for a period up to 5 years) to help local governments that have incurred a significant loss in revenue, due to a major disaster, that has or will adversely affect their ability to provide essential municipal services.

The ICR collects contact information for a POC associated with the ICR, as well as information related to disaster-related losses for which the loan is requested and the information FEMA requires in order to route funds to the affected locality as part of the loan program. This PTA will extend the use of the Loan Package utilized to implement the Community Disaster Loan Program (1660-0083).

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☐ DHS employees/contractors (list components): ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?	

---

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 4 of 7

The following information is collected on local government's primary and alternate contacts:

- The individuals' name, title, signature, local government mailing address, email address, telephone numbers and fax numbers.

Financial information to include:

- The local community's name, address, telephone number, the Financial Institution's name, address, telephone number, Direct Deposit Account Number, Bank Routing Number, Claim or Payroll ID Number;
- The name and telephone number of the Financial Institution's Certifying Representative.

4(a) Does the project, program, or system retrieve information by personal identifier?	☒ No. Please continue to next question. ☐ Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	N/A
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	N/A
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
N/A	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list:

---

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 5 of 7

6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. Please describe applicable information sharing governance in place:
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

---

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 6 of 7

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Lane Raffray**
Date submitted to Component Privacy Office:	**December 4, 2014**
Date submitted to DHS Privacy Office:	December 8, 2014
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
PIA: DHS/FEMA 013 – Grant Management Programs SORN: DHS/FEMA-009 - Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs March 24, 2014 79 FR 16015	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Eric M. Leckey**
PCTS Workflow Number:	**1056653**
Date approved by DHS Privacy Office:	December 9, 2014
PTA Expiration Date	December 9, 2017

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	Form/Information Collection
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☒ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 7 of 7

	☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	**System covered by existing PIA** **DHS/FEMA 013 – Grant Management Programs**
SORN:	**System covered by existing SORN** **DHS/FEMA-009 - Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs March 24, 2014 79 FR 16015**

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

This ICR, OMB 1660-0083, is a privacy sensitive collection. PII is collected and retained in the associated forms. The forms in this collection include administrative and financial information from local governments. The information, submitted by loan applicants enables FEMA to evaluate applications and make award decisions, monitor ongoing performance and manage the flow of federal funds, and to appropriately grant closure to the loan. Without this collection, FEMA will be unable to implement its Community Disaster Loan programs. OMB 1660-0083 is covered by the DHS/FEMA/PIA-013 - Grant Management Programs PIA and DHS/FEMA-009 Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs March 24, 2014 79 FR 16015. As such, the forms associated with this ICR require e3 Privacy Act Statements to provide notice to the public that this information is part of a DHS/FEMA system of records. FEMA has already completed the e3 Statement for this ICR.