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:	**FEMA Form 516-0-1 Federal Hotel and Motel Fire Safety Declaration Form (OMB ICR No. 1660-0068)**		
Component:	Federal Emergency Management Agency (FEMA)	**Office or Program:**	U.S. Fire Administration (USFA)
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:	**September 25, 1990**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	**June 30, 2012**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	**Teressa Kaas**		
Office:	**U.S. Fire Administration**	**Title:**	Fire Program Specialist
Phone:	**301-447-1263**	**Email:**	teressa.kaas@fema.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Click here to enter text.		
Phone:	Click here to enter text.	**Email:**	Click here to enter text.

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 Federal Emergency Management Agency (FEMA), U.S. Fire Administration (USFA) uses FEMA Form 516-0-1, *Federal Hotel and Motel Fire Safety Declaration Form*. The Federal Hotel and Motel Fire Safety Declaration Form collects basic information on life-safety systems related directly to fire-safety in hotels, motels, and similar places of accommodation applying for inclusion on the National Master List (NML). The Hotel and Motel Fire Safety Act of 1990, Public Law 101-391, requires FEMA to establish and maintain a list of hotels, motels, and similar places of public accommodation meeting minimum requirements for protection of life from fire; the list is known as the National Master List (NML). The referenced law resulted from a series of deadly fires in hotels and motels, occurring in the 1970's and 1980's, with high loss of life. The information is collected and distributed through an on-line electronic database accessed through the USFA website. Information submitted voluntarily by lodging establishments is reviewed and if the criteria meet the Hotel and Motel Fire Safety Act requirements, they are given a FEMA ID number and listed in the NML database. Federal travelers and the public seeking public accommodation with provisions for life-safety from fire access the NML through the on-line database and identify lodging establishments in the area to which they are traveling.
Property owners, lodging general managers, or their designee/delegate ("applicants") complete the form by providing basic information including identification of the owner(s) of the property, the business's Employer Identification Number (EIN), and provisions for life-safety from fire. The form requests specific responses from applicants as to the installation of smoke detectors in all guestrooms of properties submitted for listing on the NML. In addition, applicants must indicate if the lodging establishment has an automatic fire sprinkler system where the building is four stories or higher. For statutory reference see Title U.S.C. § 2224-26. This collection of information and form are part of Office of Management and Budget (OMB) Information Collection Resource (ICR) No. 1660-0068.
Records are retrieved by an organization's name and not by any PII.
This is a renewal—no changes to the information collection have been made since the last version.

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	☐ This program does not collect any personally

---

[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.

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

Program collect, maintain, use, or disseminate information? *Please check all that apply.*	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?	
Business Point of Contact information includes the Property Owner, General Manager or their designee/delegate's Name; Title; Name of Organization/Business; Property/Mailing Address; Business Email Address; Business Phone Number; Business Fax Number; and may include signature.	
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.	

---

[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.

[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

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

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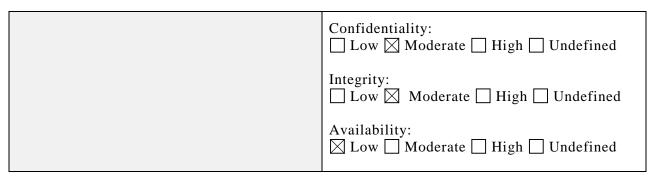**Version number: 01-2014**
Page 5 of 7

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: Click here to enter text.
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. N/A ☐ 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:

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.

[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

	Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined Availability: ☒ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	LeVar J. Sykes
Date submitted to Component Privacy Office:	Click here to enter a date.
Date submitted to DHS Privacy Office:	February 18, 2015
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
FEMA Privacy 's recommendation is that the system is a Privacy Sensitive System with the following coverage: PIA: New (Formerly covered by the DHS Contacts List PIA) SORN: N/A	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Eric M. Leckey
PCTS Workflow Number:	**1067762**
Date approved by DHS Privacy Office:	February 18, 2015
PTA Expiration Date	February 18, 2018

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	Form/Information Collection If "other" is selected, please describe: Click here to enter text.

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

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.
	☐ A Records Schedule may be required. Contact your component Records Officer.

PIA:	**New PIA is required.**
	If covered by existing PIA, please list: Click here to enter text.

SORN:	System covered by existing SORN
	If covered by existing SORN, please list:

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

The FF 516-0-1 Federal Hotel and Motel Fire Safety Declaration Form is a Privacy Sensitive System that collects business related PII of Hotel and Motel owners. FEMA collects the PII to facilitate communication between FEMA an organization/property owner. Previously this collection of information was covered by the DHS Contact List PIA, however, the general purpose of the collect exceeds the scope of the DHS Contacts List PIA. A new PIA needs to be completed for this collection.

Additionally, the FF 516-0-1 is retrieved by an organization/business name and not by the Point of Contact's PII. No SORN is required for this collection.