OFDAnet RED Files

PRIVACY IMPACT ASSESSMENT (PIA) SUMMARY

System Name: OFDAnet RED Files

Managing Office: OFDA

Date PIA Completed: August 5, 2013

OVERVIEW

USAID's Office of U.S. Foreign Disaster Assistance (OFDA) deploys personnel overseas to coordinate the U.S. Government's response to disasters. While OFDA strives to undertake all prudent safety and security measures, the risk of injury to its staff can never be entirely eliminated. OFDA has mandated the collection of Record of Emergency Data (RED) files for staff deploying on Disaster Assistance Response Teams (DARTs) (see Response Management Team Policy and Procedure, Annex E, section 4.6.10), however, DART members may choose to leave fields blank if they desire. OFDA also has staff members that regularly travel on TDY assignments who have the option to submit RED files.

The voluntary collection of RED files from all OFDA staff, in conjunction with the OFDA Critical Incident Response Plan, is intended to better prepare OFDA to assist injured staff members.

AUTHORITY FOR COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Privacy office will be assisting us with a system of record.

INFORMATION COLLECTION (WHAT)

System data for the OFDA Red File includes name, phone number, medical history, passport number, date of birth, address and a photograph.

INFORMATION COLLECTION (WHY)

Emergency contact information.

AGENCY INTENDED USE

OFDA's Safety and Security Unit (SSU) will be the custodians of OFDA staff members' RED files, all submissions and revisions of RED files will be done through this unit. Hard copies of RED files will be stored in a safe. NO ELECTRONIC COPIES WILL BE MAINTAINED. Any electronic RED files submitted to the SSU will be printed, stored in a safe, and the electronic version will be deleted. An access log will be used to record all access to the safe containing OFDAnet RED files.

Access to stored RED files, beyond the initial collection and updates by the SSU and per the permissions granted in the Authorizations section, will only be granted by the OFDA Director, Deputy Director, or their designee in emergency situations. OFDA staff members who wish their RED file to be held by a Response Management Team (RMT) when they are deployed on a DART can provide a blanket authorization to the SSU on this form, or on a case-by-case basis by sending an email request to a member of the SSU. After authorization has been obtained, the SSU will make a hard copy of the RED file and provide it to the RMT in a sealed envelope (the original will stay with the SSU).

Copies of RED files provided to the RMT will be handled in accordance with RMT policy 4.6.10 dated March 31, 2009, and will be destroyed at the conclusion of service on a DART.

Any requests to third party designees holding the RED file information of an OFDA staff member will be made by the OFDA Director, Deputy Director or their designee . Requests will be made using the most appropriate and expedient form of communication. The determination of whom and to what entities RED files will be released will be made on a case-by-case basis by the OFDA Director, Deputy Director or their designee; examples might include doctors, other USG officials and evacuation service providers.

OFDA senior staff understands that the information contained in RED files is sensitive and will give due consideration to the balance between the need for information and the privacy of the individual before releasing RED file information, in whole or in part to any outside party.

At any time, an individual can request that their RED file be destroyed, without any justification or reason given. The SSU will periodically review the RED file system and destroy any files of employees who are no longer working for, or in association with OFDA. However, it is the responsibility of the individual to inform the SSU of their imminent departure or disassociation with OFDA, regardless of the circumstances, to ensure the timely destruction of their RED file.

INFORMATION SHARING

The PSC contracts team on the support services contract along with the USAID Contracting Officer

NOTICE OF OPPORTUNITIES FOR CONSENT

The OFDA Staff may opt out of this information collection.

INFORMATION SECURITY

RED files will be stored in a safe maintained by SSU. An access log will be used to record all access to the safe containing OFDA RED files.

SYSTEM OF RECORDS NOTICE (SORN)

No, Privacy office will be assisting us with a system of record.