Privacy Impact Assessment
for the

FEMA Suspicious Activity Reporting (SAR)

DHS/FEMA/PIA-018

June 5, 2018

Contact Point
Mark Pfeiffer
Internal Investigations Branch
Fraud and Internal Investigation Division
Office of the Chief Security Officer
Federal Emergency Management Agency
202-212-2135

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
703-235-0780

Abstract

The Federal Emergency Management Agency (FEMA), a component of the Department of Homeland Security (DHS), manages a process for Suspicious Activity Reporting (SAR). This process, assigned to FEMA's Office of the Chief Security Officer (OCSO), is designed to collect, investigate, analyze, and report suspicious activities to the Federal Bureau of Investigations (FBI) Joint Terrorism Task Force (JTTF), Federal Protective Service (FPS), and/or other federal, state, or local law enforcement authorities required to investigate and respond to terrorist threats or hazards to homeland security. FEMA is conducting this privacy impact assessment (PIA) because this SAR process collects, maintains, and uses personally identifiable information (PII). FEMA OSCO is updating and replacing the DHS/FEMA/PIA-018 FEMA Suspicious Activity Reporting, dated September 9, 2011, to reflect that FEMA's SAR process will remain at the agency level and will not be centralized under a DHS wide SAR system.

Overview

FEMA's SAR process helps FEMA OCSO contribute to FEMA's mission to "support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards." More specifically, FEMA OCSO will collect, maintain, use, and retrieve records on individuals who report suspicious activities, individuals reported as being involved in suspicious activities, and individuals charged with the investigation, analysis, and appropriate handling of suspicious activity reports. FEMA's OCSO, Fraud and Investigations Unit, manages this process.

FEMA OCSO collects SAR information from individuals inside and outside of FEMA through an OSCO-operated toll free telephone number (866-847-7056), a tip line email address (FEMA-OCSO-Tipline@fema.dhs.gov), the FEMA website (www.fema.gov), and directly to FEMA personnel staffed at disaster locations, joint field offices, regional offices, and other FEMA locations. These reports are collected by FEMA in a brief narrative and include the suspected activity and contact information of the person reporting the incident. Upon receipt of the reported incident, FEMA OCSO assigns a case number for tracking in FEMA OCSO's SAR case management spreadsheet, and then assigns each case to a FEMA OCSO investigator and/or analyst. The FEMA OCSO investigator and/or analyst may contact the person reporting the suspicious activity to conduct additional research as necessary to verify and validate the information provided.

The result of this conversation and additional research is documented in a FEMA OCSO Offense/Incident Report, which typically falls into one of the following three categories: 1) FEMA OCSO investigator and/or analyst determines that the report is unfounded; 2) FEMA OCSO investigator and/or analyst determines that the report does not have a nexus to terrorism or hazards to homeland security but does require transfer to federal, state, or local law enforcement authority;

or 3) FEMA OCSO investigator and/or analyst determines that the report meets the Information Sharing Environment (ISE) Functional Standard[1] for determining a nexus to terrorism, so he or she notifies the FBI JTTF by entering the appropriate SAR information and data into the FBI e-Guardian system[2] where it can be accessed, evaluated, and analyzed by authorized personnel, partners, and stakeholders outside the Department under the Nationwide SAR Initiative (NSI).

Following necessary transfer to the appropriate authorities, FEMA's OCSO investigator and/or analyst concludes the investigation by entering the analysis into a paper-based FEMA OCSO Offense/Incident Report, scanning a copy of the Offense/Incident Report to be stored on the OSCO shared-drive, updating the case management spreadsheet, and filing the paper copy in a secure location within FEMA OCSO offices. To reduce any risk of unauthorized access, FEMA SARs are secured in a room monitored by FEMA OCSO investigators and analysts. Electronic files maintained in the FEMA OCSO shared-drive are protected from unauthorized access through appropriate technical safeguards such as two-part user authentication to access any FEMA system on a secured network.

FEMA's SAR process is authorized and governed by 44 CFR Chapter 2 "Delegation of Authority;" 42 U.S.C. § 5196(d); Executive Orders 12333 and 13388; 40 U.S.C. § 1315(b)(2)(F); 6 U.S.C. § 314; the Homeland Security Act of 2002, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the National Security Act of 1947, as amended; and FEMA Manual 1010-1 "Federal Emergency Management Agency Missions and Functions."

FEMA SAR information may be shared during the course of an investigation or further analysis by a FEMA OCSO investigator and/or analyst. As outlined above, this may occur when information is passed to the FBI JTTF, FPS, or to other federal, state, or local law enforcement authorities for appropriate action. All information shared is deemed For Official Use Only (FOUO) or Law Enforcement Sensitive (LES) and is governed by Executive Order 12958 and 13292. Any unauthorized disclosure of FOUO or LES information may constitute a violation of Title 18, §§ 641, 793, 798, 952, and 1924.

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?

FEMA's authority to collect SARs and conduct investigations is permitted by, but not limited to, the following legal acts: 44 CFR Chapter 2, Delegation of Authority, and FEMA Manual 1010-1. Other authorities include: 42 U.S.C. § 5196(d); Executive Orders 12333 and

[1] ISE SAR Functional Standard version 1.5.5 *available at* https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf.
[2] For information on e-guardian, *see Federal Bureau of Investigation Privacy Impact Assessment for the eGuardian System, available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/eguardian-threat.

13388; 40 U.S.C. § 1315(b)(2)(F); 6 U.S.C. § 314, the Homeland Security Act of 2002, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; and the National Security Act of 1947, as amended.

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

The following DHS SORNs apply:

- *For FEMA SARs:* DHS/FEMA - 012 Suspicious Activity Reporting Files System of Records September 28, 2011 76 FR 60067
    - Final Rule for Privacy Act Exemptions January 10, 2012 77 FR 1387

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

FEMA's OCSO SAR process utilizes existing FEMA tools, applications, and systems rather than a new system itself. For that reason, no system security plan is required or has been completed.

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

Yes, Pursuant to National Archives and Records Administration (NARA) Schedule Number N1-311-99-6, Items 1, 2, and 3, files containing information or allegations that are of an investigative nature but do not relate to a specific investigation are destroyed when five years old. Investigative case files that involve allegations made against senior agency officials, attract significant attention in the media, attract congressional attention, result in substantive changes in agency policies and procedures, or are cited in the OIG's periodic reports to Congress are cut off when the case is closed, retired to the Federal Records Center (FRC) 5 years after cutoff, and then transferred to NARA 20 years after cutoff. All other investigative case files except those that are unusually significant for documenting major violations of criminal law or ethical standards by agency officials or others are placed in inactive files when case is closed, cut off at the end of fiscal year, and destroyed 10 years after cutoff.

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.

FEMA's OCSO SAR process does not trigger the requirements of the PRA because collection is by voluntary submittal from individuals inside and outside of FEMA. Any collection

from the public falls under 5 CFR 1320.4(a)(4), and is thus exempted from requirements of the PRA.

Section 2.0 Characterization of the Information

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

FEMA's OCSO SAR process collects information about suspicious activities and individuals made by individuals inside and outside of FEMA. This information is supplemented by additional investigation and analysis by FEMA OCSO investigators and/or analysts. This information is captured in a FEMA OCSO Offense/Incident Report and scanned and stored on the FEMA OCSO shared-drive. This report enables the collection of standardized information about individuals who report suspicious activities, individuals reported as being involved in suspicious activities, and individuals charged with the investigation, analysis, and appropriate handling of suspicious activity reports. The information collected is consistent for each group and includes the following:

- Case/Incident Number;
- Name (first, middle, last);
- Address (number, street, apartment, city, state);
- Age;
- Sex;
- Race;
- Injury code if applicable;
- Signature (Investigator, Analyst, or Law Enforcement Officer (LEO));
- Jurisdiction;
- Telephone numbers (home, business, or cell);
- Other contact information (e.g., email address); and
- Property information (name, quantity, serial number, brand name, model, value, year, make, color, identifying characteristics, and registration information).

FEMA's OCSO investigators and analysts also utilize a commercial source of information called LexisNexis/Choice Point to verify the identity information collected from reporting or suspicious individuals. In addition, FEMA OCSO investigators and analysts query the FBI e-Guardian system to identify any additional relevant information.

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

As defined in Section 2.1, FEMA OCSO investigators and analysts obtain information directly from individuals, from other government and commercially available systems, and also from other law enforcement entities to complete their investigations and analysis.

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

As defined in section 2.1, FEMA's OCSO utilizes LexisNexis/Choice Point to verify the identity information collected from reporting or suspicious individuals.

2.4 Discuss how accuracy of the data is ensured.

Accuracy of the information is the responsibility of the individual providing the information to FEMA. FEMA OCSO investigators and analysts validate the data and information through the analytic process of their investigation utilizing the sources of information described in Section 2.1. A FEMA OCSO supervisor, within the Fraud and Investigation Unit, reviews all Offense/Incident Reports for completeness, safety issues, and specificity prior to dissemination of that information to the FBI JTTF, FPS, or other federal, state, or local law enforcement authority. Additionally, PII contained in the Offense/Incident Reports may be reviewed for accuracy by the individual from whom the PII is collected when not otherwise prohibited by law.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information may not be accurate or timely because it is not always collected directly from the individual involved.

Mitigation: This risk is partially mitigated. FEMA contracts with a third party identity verification service that is obligated by contract to provide accurate data. The assumption is made initially that the data is accurate for this reason. FEMA periodically performs quality control reviews on previous reports to verify data accuracy. Investigations and verifications of reported information are completed in a diligent and complete manner. This is accomplished through employee training on responsible steps to ensure that sufficient and relevant details have been captured, and that proper legal authorities are notified to mitigate any potential hazard. Sources of investigative information are documented in sufficient detail to provide a basis for assessing its reliability

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

FEMA's OCSO SAR process collects information about suspicious activities and individuals made by individuals inside and outside of FEMA. This information is supplemented by additional investigation and analysis by FEMA OCSO investigators and/or analysts. This information is captured in a FEMA OCSO Offense/Incident Report and scanned and stored on the FEMA OCSO shared-drive. This report enables the collection of standardized information about individuals who report suspicious activities, individuals reported as being involved in suspicious activities, and individuals charged with the investigation, analysis, and appropriate handling of suspicious activity reports.

Following this process, one of three things will occur: 1) FEMA OCSO investigator and/or analyst determines that the report is unfounded; 2) FEMA OCSO investigator and/or analyst determines that the report does not have a nexus to terrorism or hazards to homeland security but does require transfer to federal, state, or local law enforcement authority; or 3) FEMA OCSO investigator and/or analyst determines that the report meets the Information Sharing Environment (ISE) Functional Standard for determining a nexus to terrorism, so he or she notifies the FBI JTTF by entering the appropriate SAR information and data into the FBI e-Guardian system where it can be accessed, evaluated, and analyzed by authorized personnel, partners, and stakeholders outside the Department under the NSI.

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. There are no other Departmental components that are assigned roles and responsibilities within this process.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of misuse or unauthorized access to the information.

Mitigation: To mitigate this risk, access to background checks are conducted on all personnel that may access FEMA investigatory records and only those FEMA OCSO personnel with the appropriate roles may access SAR records. FEMA SAR records are controlled by limiting access to records, which are secured in a room monitored by FEMA OCSO investigators and

analysts. The case managers maintain a manifest of all FEMA OCSO personnel and their roles/titles.

Section 4.0 Notice

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

Notice is not typical due to the fact that SAR reporting frequently results in escalation to law enforcement agencies, and any release of this information could adversely affect or jeopardize investigative activities. Furthermore, all information shared is deemed FOUO or LES and is governed by Executive Orders 12958 and 13292. Any unauthorized disclosure of FOUO or LES information may constitute a violation of Title 18, §§ 641, 793, 798, 952, and 1924.

The public is provided notice via this PIA and the SORNs listed in section 1.2. When an individual contacts FEMA about a suspicious activity, the FEMA OCSO investigator or analyst also provides additional notice to the individual.

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

SARs received inside or outside of FEMA typically come voluntarily. Individuals are providing their consent for the use of the information provided.

Individuals being investigated by FEMA OSCO investigators are not given the opportunity to consent or decline to provide information or opt out of the investigation.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that information could be used in a manner inconsistent with the established DHS/FEMA privacy policies.

Mitigation: FEMA OCSO does not collect more information than is needed for the SAR investigation and analysis and does not share information with other agencies or jurisdictions that do not have a need-to-know. Access is strictly limited to authorized staff that requires access to perform their official duties. Information is also protected from unauthorized access through appropriate technical safeguards such as two part user authentication to access any FEMA system on a secured network.

Privacy Risk: There is a risk that individuals who are subjects of an SAR will not receive notice of this collection.

Mitigation: Given the nature of SAR, individuals are not provided notice as to whether they are the subject of an SAR. Providing direct notice to an individual may be harmful to intelligence or law enforcement activities. FEMA partially mitigates this risk by publishing this

PIA and the DHS/FEMA - 012 Suspicious Activity Reporting Files SORN.

Section 5.0 Data Retention by the project

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

Pursuant to National Archives and Records Administration (NARA) Schedule Number N1-311-99-6, Items 1, 2, and 3, files containing information or allegations which are of an investigative nature but do not relate to a specific investigation are destroyed when five years old. Investigative case files that involve allegations made against senior agency officials, attract significant attention in the media, attract congressional attention, result in substantive changes in agency policies and procedures, or are cited in the OIG's periodic reports to Congress are cut off when the case is closed, retired to the Federal Records Center (FRC) 5 years after cutoff, and then transferred to NARA 20 years after cutoff. All other investigative case files except those that are unusually significant for documenting major violations of criminal law or ethical standards by agency officials or others are placed in inactive files when case is closed, cut off at the end of fiscal year, and destroyed 10 years after cutoff.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that FEMA OCSO will maintain incident and personnel information longer than is needed and thus increase FEMA OCSO's vulnerability to a major privacy incident.

Mitigation: FEMA OCSO's policies and procedures for expunging data, including records pertaining to approved and unapproved applications, at the end of retention period are consistent with NARA policy guidance. These procedures are documented by the FEMA Records Officer and follow NARA's General Records Schedule (GRS) guidelines, including the submittal of SF 115 forms to NARA. Electronic records are destroyed in accordance with the same NARA GRS that applies to hard paper copies.

Section 6.0 Information Sharing

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 OCSO investigators and analysts may share information with the FBI JTTF, FPS, and other federal, state, and local law enforcement authorities; however, FEMA OCSO investigators and analysts only share information with appropriate authorities who have a need to know and only when FEMA OCSO investigators and analysts deem it appropriate to do so. All information shared is deemed FOUO and LES and is governed by Executive Orders 12958 and 13292. Any unauthorized disclosure of FOUO or LES information may constitute a violation of Title 18, §§ 641, 793, 798, 952, and 1924.

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

Routine uses listed in the SORNs outlined in Section 1.2 allow FEMA to share information with the FBI JTTF, FPS, and other federal, state, and local law enforcement authorities. SARs may reveal activities that constitute a violation of law or otherwise require attention from law enforcement. The sharing of SARs through a standard distribution list to notify appropriate entities is compatible with the routine uses and the original purpose for collection.

6.3 Does the project place limitations on re-dissemination?

All information shared is deemed FOUO or LES and is governed by Executive Orders 12958 and 13292. Any unauthorized disclosure of FOUO or LES information may constitute a violation of Title 18, §§ 641, 793, 798, 952, and 1924.

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

FEMA OCSO investigators and analysts maintain a record of all disclosures to the FBI JTTF, FPS, and other federal, state, and local law enforcement authorities. In addition, the FBI e-Guardian system used to input SARs with a nexus to terrorism maintains a record of all reports that have been previously entered. Using this functionality within e-Guardian, FEMA can generate a list of reports provided to the FBI JTTF.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that FOUO and LES information may be lost, stolen, or compromised.

Mitigation: Information received by the FEMA OCSO investigators and analysts is not shared internally with other DHS components or externally with federal, state, or local authorities except for the reasons outlined in this PIA and the applicable SORNs. These sharing practices come with additional safeguards on the receiving end. In those instances, information is shared via hard copy printouts that are hand delivered to and signed for by authorized personnel, or registered mail, thereby reducing the privacy risks associated with transmitting sensitive personal information.

Section 7.0 Redress

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

Individuals may contact FEMA OCSO who can verbally read back the statement they provided when reporting the incident. In addition, individual members of the public may make a Freedom of Information Act (FOIA) request for copies of records from FEMA OCSO that are

relevant to that individual by using the online form on the FEMA.gov website (www.dhs.gov/dhs-foia-request-submission-form.) or by emailing a request to FEMA-FOIA@dhs.gov. FOIA requests may also be submitted through the regular mail at the following address: FEMA Information Management Division, Disclosure Branch, 500 C Street, SW, Mail Stop 3172, Washington, D.C. 20472.

These rights are provided to the extent practicable for FEMA operations. Despite being exempted under the Privacy Act, FEMA responds to any information requests on a case-by-case basis when compliance would not hinder or unduly burden FEMA operations. Each request will be evaluated and all records provided to the requestor to the extent permitted by law.

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

Individuals can contact FEMA OCSO through the toll-free hotline, via the email tip line, and by using the direct contact number provided during the course of the investigation to request corrections to erroneous information. In addition, they may also request an update to erroneous information by regular mail at the following address: FEMA Office of Chief Security Officer, Fraud and Investigation Unit, 1201 Maryland Avenue, SW, Washington, D.C. 20024.

To correct the information, FEMA's OCSO adds a supplement to the original report and updates the appropriate authorities if the changes resulted in new information.

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

Individuals are provided notice by this PIA and associated SORN. In addition, FEMA OCSO investigators and analysts provide direct FEMA OCSO contact information so that individuals reporting suspicious activity can provide additional information at a later date.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that too much or inaccurate information will be collected on individuals without their knowledge or consent to accuracy.

Mitigation: Individuals may contact FEMA OSCO or the FEMA Disclosure Branch as discussed in Section 7.1 above to access and correct information on them or provided by them.

Section 8.0 Auditing and Accountability

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

FEMA OSCO incorporates the stated practices within this PIA in their SAR Standard Operating Procedures (SOPs) and everyone who participates in the FEMA SAR process is required to attend the mandatory analyst training. Also, the FEMA OSCO Fraud and Investigation Unit

Director reviews all reports to ensure information is complete and accurate. FEMA OCSO and this process are also subject to audits from the Government Accountability Office (GAO) and DHS Office of the Chief Security Officer.

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

All DHS employees are required to take basic privacy training and the FEMA OCSO provides refresher privacy awareness training annually to their staff as it relates to law enforcement activities. In addition, all individuals who are interacting with the FEMA OSCO SAR process are required to take specialized training on the use and submission of SAR information and data.

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

As referenced in section 8.1, the case manager accessing the files has a list of authorized FEMA OSCO personnel and their roles to determine who may review case files. This list is reviewed regularly to make sure that listed individuals are authorized current employees of FEMA.

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 OSCO does not a have Memoranda of Understanding (MOU) or Information Sharing Access Agreements (ISAA) with agencies inside or outside of DHS. The information shared is deemed FOUO or LES and is governed by Executive Orders 12958 and 13292. Any unauthorized disclosure of FOUO or LES information may constitute a violation of Title 18, §§ 641, 793, 798, 952, and 1924.

Responsible Officials

William H. Holzerland
Senior Director for Information Management
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security