Privacy Impact Assessment for the

National Fire Incident Reporting System (NFIRS)

DHS/FEMA/PIA-044

June 8, 2017

Contact Point
Brad Pabody
Chief
National Fire Data Center
United States Fire Administration
Federal Emergency Management Agency
(301) 447-1340

Reviewing Official
Jonathan Cantor
Chief Privacy Officer (Acting)
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), United States Fire Administration (USFA), National Fire Programs (NFP), National Fire Data Center (NFDC) owns and operates the National Fire Incident Reporting System (NFIRS). NFIRS is an information technology (IT) system that collects and maintains data associated with emergency responses by fire departments nationwide to analyze and measure the national fire problem as directed by USFA. FEMA is conducting this Privacy Impact Assessment (PIA) because NFIRS may contain personally identifiable information (PII) of fire casualties, property owners, fire and emergency medical service personnel, and other persons involved in the incidents.

Overview

The USFA was established as a result of the Federal Fire Prevention and Control Act of 1974, and its mission is to administer fire prevention and control programs, supplement existing programs of research, training, and education, and encourage new and improved programs and activities by state and local governments. Furthermore, Sections 9(a) and 9(b) of the Act authorize the USFA Administrator to operate directly, or through contracts or grants, an integrated, comprehensive method to select, analyze, publish, and disseminate information related to prevention, occurrence, control, and results of fires of all types. Specifically, it enables the USFA to: 1) gather and analyze information on the magnitude of the nation's fire problem, as well as its detailed characteristics and trends; 2) develop uniform data reporting methods; and 3) encourage and assist state agencies in developing and reporting data.

To fulfill its mission, USFA established and operates the NFIRS. NFIRS is an IT system comprised of a database, client-based tools, and web-based tools. NFIRS provides USFA a mechanism using standardized reporting methods to collect and analyze fire incident data at the federal, state, and local levels. The objectives of NFIRS is to: 1) help state and local fire departments develop fire reporting and analysis capability for their own use to focus on current problems, predict future problems in their communities, and measure whether their prevention and education programs are working; and 2) obtain data that can be used to more accurately assess and subsequently combat the fire problem at a national level.

The NFIRS system provides state and local fire department users a suite of standard forms and output reports that can be run to aggregate NFIRS data at the local fire department level or alternatively at the state level. These output reports do not include any PII. At the national level, FEMA/USFA uses analytical statistical tools to aggregate and analyze NFIRS data. NFIRS analysis and reports are used to determine fire trends and the top causes of fires on an annual basis; answer questions about the nature and causes of fire-related injuries, deaths, and property loss; and

determine where fires occur the most often. The results are used for prevention in local, state, and national programs and to drive legislation for programs such as home detectors and sprinklers. Furthermore, NFIRS data may be used by local, state, and national government agencies to monitor fire problems in consumer products.

The USFA developed a standard NFIRS package that includes incident and casualty forms, user manuals, computer software and procedures, documentation, and National Fire Academy training courses for using the system. Incident data from local fire departments can be directly submitted to NFIRS through the client-based or web-based data entry interface. Incident data can also be forwarded via paper or electronic files to a state program office, where the data is validated and consolidated into a state-owned database and aggregated statewide data is then periodically transmitted to NFIRS. NFIRS users may be from fire department and program staff in state and local governments, the Department of Defense, the Native American Tribal Authority, and U.S. Territories.

All users must register and be given access to NFIRS. A new fire department user registers his/her information on the www.nfirs.fema.gov site using the NFIRS web registration tool. The user's NFIRS State Program Manager must approve the account and give the user specific permissions for the various NFIRS applications. Once the user has an account and appropriate permissions, he or she can access the web tools and services necessary for fire personnel to report, submit, and maintain incident information. The data consists of detailed information about fires, casualties, hazardous materials, Emergency Medical Services (EMS) response, wild land fires, arson fires, and the numbers and types of apparatus and personnel used to mitigate these incidents. The information submitted in the reports may include the PII of individuals involved in responding to fire related incidents and casualties from the fire; however, that information is not used for any national level analysis or reports.

After a fire incident occurs, fire departments collect information associated with the incident for reporting purposes. This includes general information regarding the nature of the incident and response effort, such as the size or cause of the fire, and type of technology or tool that was used in the response. During this time, fire departments may also collect PII and demographic data of individuals involved in or impacted by the incident, such as name, address of the owner of the property where a fire incident occurs, or age, race, and gender. Additionally, fire departments may collect and report information associated with the personnel involved in the fire response. This information is collected to document the entire fire incident and to track patterns of fire and prevention efforts. Some departments may also provide documentation to victims of fire incidents who have a need to submit loss information to their insurance companies. The demographic information is used as aggregate data in reports produced at the local, state, and national level. Race, age, and gender information are not associated with the individuals in the reports.

NFIRS contains standard forms with data fields that users can use to collect and report information directly into the system. When users enter NFIRS they can choose which form or module to complete, depending on the specific incident. The fire department users responding to an incident collect the information directly from the individuals present at the scene. Additionally, the forms have a remarks section where PII may incidentally be documented. PII is protected by user group security built into the NFIRS system so that only the local departments and states to which the data belongs have access to it. The data collected and input into NFIRS by the local fire departments and states belongs the specific users; FEMA/USFA does not have access to this information other than those staff who maintain the system. Therefore, historical data including PII are kept indefinitely for use in longitudinal analyses by those fire departments that own the data. For many departments that participate in NFIRS, the USFA database is the only method they have for electronic storage and retrieval of the records. Those records need to be maintained to conduct long range studies and trend analysis. The information that is entered into NFIRS is compiled and stored in the system database. FEMA/USFA exports a subset of NFIRS data fields annually from the production database for analysis purposes. FEMA/USFA does not include any PII data fields in the export; it only exports aggregated data. The data is loaded into statistical software and analyzed with custom queries and reports.

Participation in NFIRS is voluntary and use of the system is provided as a service to participating fire departments. This service is provided to encourage fire department reporting because for many smaller, mostly volunteer fire departments, it may be the only method available for documenting their incident responses. Many departments cannot afford to buy software programs so the USFA provides this service allowing those departments to collect what they need at the local level, which in turn, gives the states and the USFA the additional data needed to address the fire problem at the state and national levels. If USFA were not able to provide that service, many of those departments would be forced to go back to paper based systems or their own home-grown system resulting in a potential loss of data needed to track and address the fire problem in the United States. NFIRS is a voluntary system, so USFA must provide incentives for local fire departments to participate. The largest incentive is to collect data that fire departments need at the local level.

The primary privacy risk associated with NFIRS is unauthorized access to or use of PII. This privacy risk is mitigated by employing group security measures that limits access of PII to only the data owners. A user cannot access another fire department's data. PII is collected and used under the authority of the users. Data may be exported from NFIRS to compile reports; however, the reports only contain aggregated data. They do not contain any PII. FEMA/USFA personnel do not have access to any PII other than personnel who administer the system for system operation and maintenance purposes. Those personnel do not perform searches on PII.

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?

The Federal Fire Prevention and Control Act of 1974 (Public Law 93-498) establishes USFA to administer fire prevention and control programs; supplement existing programs of research, training, and education; and encourage new and improved programs and activities by state and local governments. Section 9(a) of the Act authorizes the USFA Administrator to operate directly or through contracts or grants, an integrated, comprehensive method to select, analyze, publish, and disseminate information related to prevention, occurrence, control, and results of fires of all types.

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

FEMA does not retrieve incident response information in NFIRS using personal identifiers, and therefore does not require SORN coverage. FEMA/USFA only uses the information in a manner that is compatible with the original purpose of collection, which is to collect and maintain data associated with emergency responses by fire departments nationwide to analyze and measure national fire problems as directed by USFA. FEMA may retrieve system access information by PII such as by username or the user's name. FEMA's collection, use, and sharing of system access information has coverage under the DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012).

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

A System Security Plan was completed October 24, 2014, and a one year Authority to Operate (ATO) for NFIRS was granted on September 8, 2014. A two year extension of this ATO was approved by the CIO on July 6, 2015, making the current expiration date July 8, 2017.

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

NARA General Records Schedule GRS 4.3, item 020, Electronic Input/Source Records.

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.

OMB No. 1660-0069, National Fire Incident Reporting System (NFIRS) Version 5.0., expiration – April 30, 2019.

Section 2.0 Characterization of the Information

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

Fire departments may collect the following information from individuals impacted or involved in the fire incident:

- Name(s) of homeowners or business owners;
- Addresses of homes or businesses impacted by the fire incident;
- Phone numbers;
- Names of causalities (injured or deceased);
- Date of birth (only used to calculate age);
- Race/ethnicity;
- Age; and
- Gender.

The fire department personnel collects the following information associated with fire incident response:

- Names, including officer in charge, member creating the report, and others;
- Names of casualties during the response;
- Rank or position;
- Phone numbers;
- Email addresses; and
- Personnel IDs.

The following information is maintained in the system pertaining to system access:

- User first and last name;
- Username;
- Password;
- User's email address; and
- User's contact phone number.

PII may also be incidentally captured in the remarks section of the tool. The remarks box is a free text box where fire departments can provide a narrative on the incident. This information is only accessible by the specific fire department owner of the information. While certain FEMA system administration personnel have the capability to access all information within the database, information is not extracted from the remarks section.

Additionally, fire departments also collect information associated with the nature of the fire incident and the response effort. This information includes detailed information about fires, hazardous materials, EMS response, wild land fires, arson fires, and the numbers and types of apparatus used to mitigate these incidents.

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

Data is provided to NFIRS by fire department and program staff in state and local governments, the Department of Defense, the Native American Tribal Authority, and U.S. Territories. Local fire departments complete incident, casualty, and optional reports for fires and other incident types as they occur. The local fire departments collect PII from persons involved in an incident directly from those individuals or other knowledgeable individuals on the scene of an incident.

Some incident data are received from state systems that collect fire incident data from local fire departments within the state. Incident data is forwarded via paper forms or electronic files to a state program office where the data is validated and consolidated into a single database and aggregated statewide data are transmitted to NFIRS periodically in electronic form.

State and USFA NFIRS Program Managers collect NFIRS user registration information directly from individuals.

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

No. NFIRS does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Each state program and the fire department user is responsible for ensuring the accuracy of the NFIRS data. Any PII within NFIRS is assumed to be accurate, as it is collected by the users (i.e., fire departments) directly from the owners of the information. USFA relies on the users (i.e., fire departments) to ensure the information is accurate. FEMA/USFA does not modify data in the NFIRS. Rather, it hosts the system as a service to the fire departments and only uses the non-PII data to conduct statistical and trend analyses on fire incident events.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that NFIRS may collect, maintain, or use erroneous or inaccurate information on individuals entered by the fire department collecting the data.

Mitigation: This risk is partially mitigated. FEMA limits the places where individuals could provide PII. FEMA also includes language in the NFIRS user guide that cautions users against adding any PII in the remarks section of the form.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Fire departments collect and use this information to document and analyze the incident. Collectively, the information is used to determine fire trends and the top causes of fires on an annual basis, answer questions about the nature and causes of fire-related injuries, deaths, and property loss, and determine where fires occur the most often. Information such as race, age, and gender are only used for statistical analysis and to report on aggregated data. Fire departments may collect PII of the individuals impacted by the fire incident in order to provide documentation to those who need to submit loss information to their insurance companies. FEMA/USFA only exports and uses aggregated data to compile reports on fire trends; FEMA does not include PII in any of the exports, studies, or any other analysis of the data.

NFIRS user information is collected to provide access to the system. There are no other uses for this information.

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.

FEMA/USFA does use technology to conduct electronic searches, queries, and analyses in an electronic database to discover or locate a predictive patterns or trends in fire losses. These searches and queries do not include fields containing PII, nor do they seek to predict behavior of individuals.

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

No. There are no other DHS components with assigned roles and responsibilities within NFIRS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that NFIRS data may be disclosed to unauthorized individuals.

Mitigation: This privacy risk is mitigated by establishing clear access controls for NFIRS users. This includes assigning users to specific user groups that defines the NFIRS data to which the user has access. NFIRS users are also assigned one or more permission types for system functions. In other words, NFIRS users are only given permission to access their own data; they cannot access any other fire department data.

Privacy Risk: There is a privacy risk that NFIRS data may be used in a manner that is inconsistent with the purpose of collection.

Mitigation: This risk is mitigated because all NFIRS users are required to complete NFIRS system training after initial registration. Local fire departments will only use the information to support their reporting needs and requirements. FEMA/USFA personnel do not have access to any PII other than personnel who administer the system for system operation and maintenance purposes. Those personnel do not perform searches on PII data. FEMA only exports non-PII aggregated data for reporting purposes.

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.

FEMA provides notice through the publication of this PIA. Additionally, the fire department personnel provide verbal notice to the individuals at the time of information collection. Each fire department operates under their own specific authorities and FEMA is just one of the many entities with which the fire departments share information. Since each fire department collects information under its own authority, FEMA does not provide guidance or standards on how the verbal notices are conducted.

FEMA provides notice to individuals who are NFIRS users via a link to a security and privacy statement in the footer of each page of www.nfirs.fema.gov and reporting.nfirs.fema.gov.

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

NFIRS does not directly collect information from individuals in the general public or fire and emergency medical personnel who are involved in incidents. Any methods for individuals to exercise the right to consent to particular uses of information or decline to provide information are controlled by the fire departments that collect the data.

During the user registration process, NFIRS users consent to the collection and use of their information as it is required in order to grant access. Declining to provide or not consenting to use of the user's personal information would result in FEMA not being able to provide access the NFIRS system.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals may be unaware that when they provide information to their local fire department, their PII is being placed in a FEMA system.

Mitigation: Other than through general notice by the publication of this PIA, FEMA has not mitigated this risk. FEMA does not direct or authorize the information collection; this information collection is directed and conducted by the fire departments under their own authorities. Since the fire departments own the information and may have additional uses for the information outside the scope of this sharing with FEMA, the fire departments provide verbal notification at the time of information collection. FEMA does not provide guidance or standards to fire departments regarding what is considered sufficient notice.

Section 5.0 Data Retention by the project

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

The data is maintained indefinitely unless removed by fire departments that own the data. In order for the system to be useful to local departments for analysis, historical data, including PII, may be kept indefinitely for use in longitudinal analyses by those fire departments that own the data. As the data owners, the state and local fire departments are responsible for following their own records retention policies. For many departments that participate in NFIRS, the USFA database is the only method they have for electronic storage and retrieval of the records. Those records also need to be maintained to conduct long range studies and trend analysis at the local level.

PII, such as name and address of the owner of the property where a fire incident occurs, are collected by the local departments for their use. It is not used at the state or federal levels. Such data is used locally for insurance purposes and for tracking patterns of fire and prevention efforts. PII is protected by user group so that only the local departments and states to which it belongs have access to it. The data in NFIRS belongs to the departments and states, and therefore, historical data including PII may be kept indefinitely for use in longitudinal analyses.

The Electronic Data Processing (EDP) series in the FEMA Records Disposition Schedule also applies to NFIRS and the information maintained in the system pertaining to system access. The FEMA EDP series schedule is taken directly from the NARA General Records Schedule 4.3, item 020, Electronic Input/Source Records.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: A privacy risk associated with this system is that FEMA may maintain the information collected for a longer period than is necessary.

Mitigation: This risk is partially mitigated. FEMA only controls the data it owns, which is the aggregate reporting data that does not contain PII. FEMA purges or transfers records as required by the NARA General Records Schedule GRS 4.3, item 020, Electronic Input/Source Records. Since FEMA does not own the state and local fire department records, information, including PII, is kept in accordance with the state and local records retention requirements, which may exceed the NARA retention period.

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/USFA shares information outside of DHS in two ways:

1. FEMA/USFA periodically releases non-PII data such as statistical and trend analyses results and copies of the database, not including data fields containing PII, into the public domain. Data is sent to the public domain through Open FEMA[1] and to those people that contact the program directly to request the data. The data is shared with outside organizations in order for them to conduct research to combat fire related issues, including those involved in fire prevention activities, the Consumer Product Safety Commission (CPSC), researchers, and organizations that manufacture fire safety and fire protection related products.

2. Occasionally, FEMA/USFA may share information with external entities such as the Department of Transportation (DOT) and the Consumer Product Safety Commission (CPSC), upon their request to analyze data on sources or causes of fires, etc. FEMA's Office of Chief Counsel reviews the requests and provides written authorization (or denial). In the authorization letter, FEMA specifies the Terms of Use to include: obligation to satisfy requirements of the Privacy Act, maintain confidentiality of the data, and to stipulate that the data is not to be used for any other purpose than what is described in the authorization letter. These precautions are taken when these federal organizations request the remarks field. While the remarks field is not designed to collect PII, and fire departments are cautioned against using it for such purposes, these confidentiality agreements are put in place in the event that a fire department may have inadvertently included PII in the remarks section.

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

FEMA does not retrieve incident response information in NFIRS using personal identifiers, and therefore does not require a SORN. However, in the event that information is requested by external entities, FEMA will document this sharing in a letter to the organization or execute an

[1] Open FEMA offers several ways for the public to receive automatic updates on press releases, disaster declarations, FEMA's latest blog posts, and information from our partners. For more information click the following link: https://www.fema.gov/openfema

information sharing and access agreement, such as a Memorandum of Understanding (MOU). FEMA/USFA only shares information in a manner that is compatible with the original purpose of collection, which is to collect and maintain data associated with emergency responses by fire departments nationwide to analyze and measure national fire problems as directed by USFA.

6.3 Does the project place limitations on re-dissemination?

Yes. FEMA documents all information sharing with external entities through letters to the organization or MOUs. The agreements specify Terms of Use, including placing limitations on re-dissemination of information and further disclosure of information.

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

Requests for information within NFIRS are made to the FEMA Disclosure Office who maintains the accounting of what records were disclosed and to whom under the Privacy Act and Freedom of Information Act.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: A privacy risk associated with this system includes information being shared for purposes other than those for prevention and statistical purposes.

Mitigation: This privacy risk is mitigated by FEMA limiting its information sharing to only those organizations that have an official need to have the information, and for the stated purpose and use for the original collection. Sharing will only be granted pursuant to receiving a written request from the organization. And the request must include the purpose. This will allow FEMA to verify that the requesting organization's intended purpose and use is in alignment with the purpose for the original collection.

Privacy Risk: There is a risk that FEMA may inadvertently share PII that may appear in the remarks section.

Mitigation: This risk is partially mitigated. In the NFIRS user guide, FEMA discourages individuals from providing PII in the remarks section. However, FEMA does not have a technical solution in place to redact PII put into the remarks section, so any PII in the remarks section would be shared.

Section 7.0 Redress

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

Individuals can contact the local fire department to access their information. Additionally, an individual can access his or her information through a Freedom of Information Act (FOIA) request submitted to the FEMA Disclosure Office. Such requests should be sent to: FEMA Disclosure Office, 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?

Individuals can contact the local fire department to access and correct inaccurate information. The NFIRS system has mechanisms in place that allow fire departments to update their records.

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

Notification is provided through this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk associated with NFIRS because the system could have inaccurate information and if an individual makes a request to correct the information, FEMA is not able to correct it.

Mitigation: FEMA is not able to mitigate this risk. Fire departments are the owners of the information, and share their information with FEMA (NFIRS). Any requests for redress must be made to the fire department that owns the information.

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?

Access controls measures are in place to ensure that users only have access to their respective group data. Fire department users only use the information in accordance with their own authorities. Furthermore, NFIRS generates audit records for a list of audited events content sufficient in detail to facilitate the reconstruction of system events. Accordingly, if compromise or malfunction occurs or is suspected the audit logs will serve as the basis in identifying the issue and cause. NFIRS audit logs contain, at a minimum, the following information:

- Identity of each user and device accessing or attempting to access the information system;
- Time and date of the access and the logoff;
- Activities that might modify, bypass, or negate information security safeguards;
- Security-relevant actions associated with processing; and
- All activities performed using an administrator's identity.

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 receive initial and annual privacy training. Additionally, FEMA information technology system users are required to take initial and annual security training to ensure their understanding of proper handling and securing of sensitive information.

For NFIRS users that are not FEMA employees or contractors, requirements for privacy training are determined by the state or local jurisdiction of the fire department collecting the 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?

A NFIRS user is assigned to a user group that defines the NFIRS data to which a user has access. User groups are hierarchical with parent-child relationship. The user has access to data that is at or below the level of the user group to which the user is assigned (i.e., a user assigned to District X will have access to aggregate District X data as well as data for all of the fire departments within District X). The user groups are defined by each State NFIRS Program Manager; typical groups are at the state, county, district, or fire departments level. The State NFIRS Program Manager is responsible for assigning users to user groups as well as assigning user permissions.

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?

Any Information Sharing Agreements (ISA), MOUs, new uses of the information, or new access to the system by organizations within DHS and outside, requires an MOU and/or ISA. The agreement will be developed by the System Owner and the FEMA Office of the Chief Information Officer. Then it will be fully vetted through the FEMA IT Security Branch, FEMA Privacy Officer, and Office of Chief Counsel prior to sending to the DHS Privacy Office for formal review and clearance.

Responsible Officials

William Holzerland
FEMA Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security.