



Privacy Impact Assessment
for the

National Flood Insurance Program Information Technology System

DHS/FEMA/PIA-011

October 12, 2012

Contact Point

Edward Connor

**FIMA Deputy Associate Administrator for Federal Insurance
Federal Emergency Management Agency
Department of Homeland Security
(202) 646-3429**

Reviewing Official

Jonathan R. Cantor

**Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717**



Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) Federal Insurance and Mitigation Administration (FIMA) National Flood Insurance Program (NFIP) owns and operates the NFIP Information Technology System (ITS). The NFIP ITS processes flood insurance policies and claims, specifically, policies and claims from the FEMA Direct Servicing Agent (DSA) contractor on behalf of the NFIP and by Write Your Own Companies (WYO) that sell and service flood insurance policies. An NFIP flood insurance policy can be obtained directly from a DSA through a licensed insurance broker or from WYOs. Since 1983, participating insurance companies have delivered and serviced NFIP policies in their own names, through the “Write Your Own” arrangement. The policy coverage and premiums do not differ if purchased from the DSA or WYOs. FEMA is conducting this Privacy Impact Assessment (PIA) because NFIP ITS collects, uses, maintains, retrieves, and disseminates personally identifiable information (PII) about individuals who purchase, as well as those who process, flood insurance policies from NFIP and individuals requesting access to the system.

Overview

Congress created the NFIP, through the National Flood Insurance Act of 1968, 42 U.S.C. §§ 4001- 4129. The program was established in response to the rising cost of taxpayer funded disaster relief for flood victims and the increasing amount of damage caused by floods. FIMA manages the NFIP and oversees the insurance, floodplain management, and mapping components of the program.

Approximately 20,000 communities across the United States and its territories participate in the NFIP by adopting and enforcing floodplain management ordinances to reduce future flood damage. Based on the communities’ compliance with these ordinances, the NFIP makes federally backed flood insurance available to property owners and renters in these communities.

The NFIP enables individuals and organizations in the participating communities to purchase insurance protection against losses from flooding. The basis for a community’s participation in the NFIP is an agreement with FEMA to adopt and enforce sound floodplain management ordinances to mitigate future flood risks to new construction, additions, repairs, and rebuilding in certain specially designated areas. The FEMA Community Information System (CIS) collects and maintains communities’ flood zone and floodplain information and maintains the official record of a community’s NFIP participation status. NFIP then makes flood insurance available to property owners and renters within the community as a means of reducing the risk of flood losses. Certain areas within these communities have a lower risk of flooding. Properties within these areas are eligible for Preferred Risk Policy (PRP) with a lower premium. Additionally, certain areas within these communities may be part of a Coastal Barrier Resource



System (CBRS) area. Properties within the CBRS area require more robust flood management safeguards in order to be eligible for flood insurance.

To help manage the NFIP, FEMA developed the NFIP ITS. FEMA previously published the National Flood Insurance Program Modernization/Business Process Improvement/Systems Engineering Management Support PIA for the NFIP IT (NexGen) system development. However, the NextGen system never went operational and NFIP has continuously used NFIP ITS. This PIA replaces DHS/FEMA/PIA-011 National Flood Insurance Program Modernization/Business Process Improvement/Systems Engineering Management Support, published on November 26, 2008.¹

The NFIP ITS collects flood insurance data from both the DSA and participating WYOs. WYOs are private insurance companies that sell and service FEMA's Standard Flood Insurance Policy (SFIP) under their own names. NFIP and private sector insurance companies execute an agreement that allows the WYOs to sell and administer flood insurance on behalf of FEMA. For individuals and organizations within NFIP compliant communities where WYOs are not available, NFIP uses contract support known as the DSA to provide flood insurance policies directly to the individual or organization on behalf of FEMA. Policy and claims information collected from the DSA and WYOs are categorized as transaction data and financial statements. Transaction data consist of policy information such as policyholder name and property address(es). Financial statements contain flood insurance premiums collected and claims paid for each property by the DSA and WYOs.

The NFIP ITS is comprised of the following major subsystems: 1) NFIP ITS Local Area Network (LAN); 2) Transaction Record Reporting and Processing (TRRP); 3) Actuarial Information System (AIS); 4) Traverse General Ledger Accounting Package (Traverse); 5) FIANet; 6) Data Exchange; 7) Data Lookup; and 8) BureauNet. In order to gain access to these systems, individuals must be approved by NFIP Contracting Officers' Technical Representative (COTR).

NFIP ITS Local Area Network (LAN) provides connectivity that allows data uploads and downloads to and from Data Exchange and TRRP in order to accomplish processing of the TRRP transaction data from the DSA and WYOs. The NFIP ITS LAN supports the following applications or software that interacts with the TRRP system: 1) Community Information System (CIS) Interface; 2) Code-1 Plus; 3) GeoStan; and 4) Geographic Information System (GIS).

CIS Interface collects flood zone and NFIP participation status communities and provides this publicly accessible information to the DSA and WYOs. The DSA and WYOs require this information to ensure that a property is within an eligible community.

¹ See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_nfip.pdf.



Code-1 Plus contains United States Postal Service (USPS)-generated address information and scans the submitted property address to verify a correct address and to ensure that FEMA has the most accurate address. If a match is made, then the USPS address is appended to the property information as the “standardized” address. If a match is not made, then an error report is generated.

GeoStan scans the submitted and standardized addresses to provide a longitude and latitude geocoding for the property. The application appends the most accurate or highest quality geocoding to the property address information.

GIS scans the address and geocoding information to determine if a property qualifies for a PRP or is within a CBRS area.

TRRP collects and maintains flood insurance data from the DSA and the WYOs and produces reports on activities related to the program. Additionally, TRRP creates and updates policy, claims, and community master files that are maintained on the NFIP ITS mainframe.

AIS uses the flood insurance data to support the annual flood insurance premium rate determination processes and *ad hoc* inquiries about actuarial data. NFIP actuaries use AIS to conduct analytical reviews of trends from the previous year in order to set insurance premium rates for the upcoming year.

Traverse uses the flood insurance data for accounting purposes, to verify correct premiums paid, and to fulfill financial reporting requirements.

FIANet is the internal application used only by NFIP users to access TRRP reports.

Data Exchange is the external web site² used by FEMA, FIMA NFIP, the DSA, WYOs, contractors, and state coordinators to upload, query, and download “real-time” TRRP data. This is the main entry point for NFIP ITS data and the primary report interface for NFIP stakeholders. Reports may be used by states for verification of appropriate insurance coverage within a state or community, or to identify areas that the NFIP may need additional marketing. Access to the reports is entity specific. For example, the state coordinator from Mississippi can only see data for that state. Also, the WYO user will only have access to their company data. Requests for access to Data Exchange are submitted to and only authorized by the NFIP COTR.

Data Lookup is a secure, internal-facing, browser-based application used only by NFIP to query TRRP data fields that are contained in existing reports to generate other reports based on specific parameters selected by the user.

² See <https://lookup.nfipstat.fema.gov>.



BureauNet is a public-facing, browser-based³ application used by the DSA, WYOs, and external NFIP stakeholders to view NFIP general information, manuals, and TRRP reports.

Typically, a property owner or renter seeks out the DSA or WYOs to purchase flood insurance. The decision to purchase flood insurance may be based on personal preference or requirement by state and/or local governments, developers, or mortgage institutions. The property owner or renter completes Form 086-0-1 *Flood Insurance Application* or Form 086-0-5 *Flood Insurance Preferred Risk Policy Application* and submits the application(s) and any supporting documentation to the DSA or WYOs along with any premium required.

On a monthly basis, the DSA and WYOs submit only the information from the application that is needed to manage the program such as policy holder name, proper address, coverage amount, and premium paid. Other information provided in the application such as building capacity and where contents are located are not needed to manage the NFIP. This information is collected by NFIP ITS via the Data Exchange system. Once NFIP ITS receives this information it scans the submitted addresses and standardized addresses to generate latitude and longitude information for the property. This geocoding information is appended to the property address information. If the system cannot validate, match, or geocode an address, an error report is generated and submitted to the DSA or WYOs. Corrected information can be updated during the next monthly reporting cycle.

Next, NFIP scans the addresses and geocoding data to determine if the property is eligible for a PRP or is in a CBRS area using the GIS application. If a property falls within the CBRS area without the proper documentation, an error report is generated and sent to the DSA or WYOs for follow up. The DSA or WYOs can dispute this error by submitting the updated appropriate additional documentation. For CBRS disputes, a request can be sent through NFIP to the United States Fish and Wildlife Service (F&WS). The F&WS then makes a final determination on whether the property is within the CBRS area. NFIP notifies the DSA and WYOs of the determination.

Once these processes have been completed, TRRP updates the policy, claims, and community master files with the updated information. Additionally, the community master file is updated with the current list of flood zone and community NFIP status information via the CIS Interface.

After the master files are updated, Traverse collects information from the policy and claims master files and updates the general ledger. Any discrepancy identified results in an error report being generated and provided to the DSA or WYOs with the policy number(s) and generic error codes.

³ See <https://bsa.nfipstat.fema.gov>.



Approved users may access both status and customizable reports through the: 1) BureauNet; 2) FIANet; 3) Data Exchange; and/or 4) Data Lookup systems. The DSA, WYOs, and NFIP personnel may request access to these subsystems.

Additionally, NFIP ITS provides non-renewed policy information submitted by the DSA and WYOs electronically through a marketing contractor to state and local governments to help market and promote the NFIP. This information includes, but is not limited to 1) insured property address; 2) insured name; and 3) the DSA and WYOs and policy numbers.

During the development and subsequent review of NFIP ITS, NFIP identified and mitigated several privacy risks associated with NFIP ITS. Generally, the privacy risks associated with NFIP ITS include: 1) individuals may not be aware that the DSA and WYOs are collecting information on behalf of NFIP, a government run program; 2) detailed flood insurance data is shared more broadly than necessary to accomplish the goal; and 3) flood insurance data is inaccurately appended as part of the initial screening process.

NFIP mitigates these risks by requiring the DSA and WYOs to provide a Privacy Act Statement as part of the flood insurance policy process, as well as publishing this PIA and related System of Records Notices (SORN) listed in Section 1.2 below. NFIP has implemented security controls to protect the PII that it collects, uses, maintains, retrieves, and disseminates. These controls include user account management procedures, audit procedures, access control procedures, and physical and environmental protection. NFIP performs regular comprehensive reviews of the DSA and WYOs data submissions. After these reviews are completed, NFIP rates the DSA and each WYO as satisfactory/unsatisfactory and provides the information as well as errors that affected the rating to each.

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 National Flood Insurance Act of 1968, as amended, 42 U.S.C. § 4001, *et seq.*, establishes the legal authority for the NFIP. The WYO program under the National Flood Insurance Act established the annual agreement by which every WYO company complies.

The Bunning-Bereuter-Blumenauer Flood Insurance Reform Act (FIRA) of 2004 enacted requirements for all new and renewal flood insurance policy transactions. The FIRA stipulates that all new and renewal policyholders for home addresses are to be sent the updated claims appeal process and an acknowledgement letter to be signed and returned as verification of their receipt of this information.

The Coordination of Wind & Flood Perils Act of 2010, as amended, establishes the legal authority for the NFIP to collect wind information. The purpose of this act is to remove the



burden of determining flood and wind loss allocation for the purpose of insurance claims from the insured and to place such burden on the entities that are responsible for the payment of such claims.

The Biggert-Waters Flood Insurance Reform and Modernization Act of 2012 reauthorizes the NFIP and its financing through September 30, 2017.

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, Section 1512, 116 Stat. 2310 (November 25, 2002), DHS/FEMA has relied on preexisting Privacy Act SORNs for the collection and maintenance of records pertaining to the NFIP, which is administered by FEMA.

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

The DHS/FEMA 003 – National Flood Insurance Program Files System of Records, 73 Fed. Reg. 77747, December 19, 2008, apply to the NFIP ITS. However, the following are additional SORNs that also relate to the data maintained on NFIP ITS:

- DHS/FEMA/Mitigation 1 – The National Flood Insurance Program Claims Appeal Process, 71 Fed. Reg. 32115, June 2, 2006, covers information collected, maintained, and disseminated related to policy holders appeal of final claim amount and decision against loss of property.
- DHS/FEMA 007 – National Flood Insurance Program Marketing Files, 73 Fed. Reg. 77793, December 19, 2008, covers information maintained and shared for the purpose of marketing NFIP to the general public.
- DHS/All 004 – General Information Technology Access Account Records System (GITAARS), 74 Fed. Reg 49882, September 29, 2009, covers information related to users who access DHS IT systems, including NFIP.

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

NFIP ITS is an operational system in the operations and maintenance phase of the DHS System Development Lifecycle (SDLC). A System Security Plan (SSP) was approved in July 2011, and an Authority to Operate (ATO) was issued on May 11, 2011.



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

Yes, the record retention schedules have been approved by the FEMA Records Officer and NARA as Authority N1-311-86-1 and N1-311-02-01.

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.

NFIP ITS information collections covered by the PRA are on the approved forms listed in Appendix A.

Section 2.0 Characterization of the Information

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

The following information is collected, used, maintained, retrieved, and disseminated by NFIP ITS:

Individual Insured Information:

- Individual's Full Name;
- Social Security Number;⁴
- Tax ID Number;
- Address(es);
- Email Address(es);
- Telephone Number(s);
- Company Name;
- Company Number;
- Request Date;
- Flood-Policy Number;

⁴ As of 2008, tax ID numbers and SSNs are no longer collected by NFIP, but any that were previously provided to NFIP are retained in the historical records.



- Wind-Policy Number;
- Insurance/Claims Data (i.e., Insurance Rate(s), Claim Amounts, etc.);
- Geographical Locations;
- Flood Zone Data;
- U.S. Fish & Wildlife (USF&W) Case Number;
- In CBRS/Out CBRS of Area Determination by Fish & Wildlife;
- Name of the CBRS System from Fish & Wildlife Services;
- Fish & Wildlife Version of the Target Property Address;
- Legal Description of Property;
- Property loss history;
- City Name of Where the Property is Located;
- CBRS Area/Unit Number (Area Number on Fish & Wildlife's Map);
- CBRS Area Declaration/Effective Date;
- Contact Information of the Fish & Wildlife Representative; and
- Generic Error Codes.

Information about the DSA, WYOs, and other Stakeholders:

- Organization Name;
- Point of Contact Full Name;
- Address(es);
- Email Address(es);
- Telephone Number(s);
- Flood-Policy Numbers;
- Wind-Policy Numbers;⁵

⁵ As of April 2012, NFIP is no longer supporting the collection of wind policy information and matching to flood policy information. Any wind-policy information that was previously provided to NFIP is retained in the historical records.



- Insurance/Claims Statistical Data; and
- Geographical Locations.

NFIP ITS User Account Information:

- Full Name;
- Addresses;
- Email Addresses;
- Telephone Number;
- User ID; and
- Temporary Password.

The above information may be used to generate statistical reports. No new information is created/generated by the NFIP ITS system.

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

The DSA and WYOs collect information from individuals seeking flood insurance and input the data into NFIP ITS to produce scheduled and *ad hoc* reports, as well as other forms of data. The DSA and WYOs provide transactional and financial statement data electronically to NFIP ITS.

FEMA collects the user account information outlined in Section 2.1 from NFIP stakeholders and NFIP personnel to allow controlled access to information within NFIP ITS and for the DSA and WYOs to submit flood insurance policy and claims information. Information is submitted using a user account request form.

The NFIP ITS receives flood zone and community NFIP participation status data on a daily basis from CIS, via web service style inquiry to CIS. The CIS data is used to update community information within the NFIP ITS community master file database, which is needed by the DSA and WYOs to determine if a property is eligible for flood insurance coverage.

NFIP ITS uses commercial geographical location data and USPS address data to help validate structure locations and addresses. This information is used by GIS to determine if a property can be considered for a PRP which allows for reduced premium or if a property is within a CBRS area. Federal regulations require additional requirements for properties within the CBRS. If a property is within a CBRS area and does not meet the requirements, the DSA and WYO must cancel the flood insurance policy and the property will be considered ineligible for flood insurance.



F&WS provides NFIP with information explaining the determination of the DSA and WYO appeals regarding a property's proximity to the CBRS area, whether it is located within or outside the CBRS area boundary, and the CBRS area effective date.

NFIP uses the approved forms listed in Appendix A of this PIA to collect information.

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

NFIP ITS uses commercial geocoding data and USPS address data to help validate structure locations and addresses. Also, NFIP uses this information to determine if a property can be covered as a PRP or if it is in a CBRS area. This reference data, purchased by NFIP, is also used to verify and validate the NFIP business transaction carried out by participating insurance companies. Information is provided to NFIP monthly on compact disc due to the amount of data and the size of the files. Geocoding and USPS address information updates are automated within NFIP ITS.

2.4 Discuss how accuracy of the data is ensured.

The forms listed in Appendix A collect information, such as name and email address, directly from the individual or his or her legal representative. NFIP assumes this information is correct. NFIP uses program-specific standard forms to ensure consistency of information collected by the DSA and WYOs. NFIP focuses on the underwriting and claims processes for property. The DSA and WYOs are responsible for the accuracy of information used in any transactions with their customers.

NFIP ITS uses commercial geocoding data and USPS address data to help validate structure locations and addresses. This reference data, purchased by NFIP, is also used to verify and validate the NFIP business transaction carried out by participating insurance companies. Information is provided to NFIP monthly on compact disc. If the application does not find a match to the submitted address, an error report is automatically generated and provided to the DSA or WYO. The DSA or WYO then researches the error and provides any corrected address information during the next monthly update to the NFIP ITS. Reports are generated by NFIP ITS to perform insurance and claims validation reviews. These reports may be reviewed against actual hardcopy insurance policy files located at the DSA or WYO.

NFIP executes periodic underwriting audits and claims re-inspections to check for operational accuracy at the DSA and WYOs.

Additionally, NFIP ITS generates and distributes property loss history reports to policyholders that include a list of prior claims and payments made to the property. The individual then provides corrections to any inaccurate information to the DSA or WYO that



maintains his or her policy. This ensures accuracy as it gives policyholders an opportunity to correct mistakes to contents of the property loss history form.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that NFIP may collect more information than is necessary for flood insurance policy setup and claim processing.

Mitigation: This privacy risk is mitigated by only collecting information required to comply with federal statute and regulations for underwriting and processing claims against flood insurance policies. Additionally, NFIP continually reviews data collection to ensure the need for data elements collected for insurance purposes. For instance, NFIP previously required the collection of SSN and Tax ID for insurance policy setup. Now, NFIP no longer requires or requests SSN or Tax ID from policy applicants and policy holders.

Privacy Risk: There is also a privacy risk of NFIP collecting inaccurate information for flood insurance policies.

Mitigation: This privacy risk is mitigated by NFIP using approved forms (listed in Appendix A) to collect information from the public for both the DSA and WYOs. These forms are collected directly from the insurance policy applicant and are maintained either by the DSA or WYO. NFIP ITS utilizes commercial geocoding data and USPS address data to verify accurate structures and addresses for policies; reviews reports based on NFIP ITS data that is validated against policy files located at the DSA and WYO locations; and provides regular policy information to policy holders requesting updates and corrections.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

NFIP ITS requires the name of the individuals and the associated address from the DSA and participating WYOs to verify the accuracy of NFIP policies and claims. This information also provides a historical and auditable record for NFIP's quality assurance, audit trail, and allows NFIP to contact and provide correspondence to individuals and organizations participating in, or requesting participation in the NFIP.

NFIP ITS collects transaction data and financial statements from the DSA and WYOs. NFIP ITS uses this information and third party software to verify property address, to determine whether property is in a CBRA area or on the 1316 Property Ineligibility Declaration⁶ list, to

⁶ Section 1316 of the National Flood Insurance Act of 1968 allows the States to declare a structure in violation of a law, regulation, or ordinance. Flood insurance is not available for properties placed on the 1316 Property List.



analyze property loss trends, generate statistical reports, and match records with other benefits and funds provided by NFIP. This information is needed to determine flood insurance eligibility, confirm current fiscal year and determine future fiscal year insurance premium rates, efficiently respond to data requests from government oversight entities, manage the DSA and WYO program, track grant Increased Cost of Compliance (ICC) payments, market the NFIP, and prevent duplication of benefits.

NFIP ITS also uses community information from CIS. NFIP ITS uses this information to generate a list of all communities that have been approved by NFIP to participate in the program. This information is needed so that the DSA and WYOs have a current list of flood insurance eligible communities.

Additionally, NFIP ITS uses information collected to create user access accounts. This is required in accordance with DHS/FEMA requirements for information technology systems and to control access of information entering and accessible through the system.

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.

NFIP ITS does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or anomaly.

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

There are no other DHS components outside of NFIP that have assigned roles and responsibilities within NFIP ITS.

3.4 Privacy Impact Analysis: related to the uses of information

Privacy Risk: There is a privacy risk that information collected and maintained in NFIP ITS may be used for purposes other than its original purpose.

Mitigation: This risk is mitigated by collecting only information needed to comply with federal statute and regulations, and fulfill the NFIP mission. NFIP ITS limits inappropriate use of the information collected by limiting access and user roles within the system to individuals who need the information to carry out the mission of the NFIP.



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.

NFIP provides notice by way of this PIA, the SORNs listed in Section 1.2, and the Privacy Act statements associated with NFIP ITS approved forms (listed in Appendix A). The DSA and WYOs inform policyholders of their privacy guidelines and practices and require policyholders to sign an acknowledgement statement as part of the policy purchase and renewal process.

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

Individuals are informed of their right to decline the sharing of their personal information by way of this PIA, the SORNs listed in Section 1.2, and the Privacy Act statements associated with NFIP ITS approved forms (listed in Appendix A). However, failure to provide the information requested may prevent property owners and renters from receiving flood insurance. Additionally, failure to provide information required to create a user account within NFIP ITS may prevent access to the system.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals apply for and maintain flood insurance through the DSA and WYOs and are not aware that this information is collected on behalf of the NFIP.

Mitigation: This privacy risk is mitigated by providing notice by way of this PIA, the SORNs listed in Section 1.2, and the Privacy Act statements associated with NFIP ITS approved forms (listed in Appendix A).

Section 5.0 Data Retention by the project

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

In accordance with NARA Authority N1-311-86-1, Items: 1A13a(1), 1A13a(2), and 2A12(2)b policy records are destroyed five (5) years following the termination of a policy. Claim records are maintained for six (6) years and three (3) months after final action, unless litigation exists. Claim records with pending litigation are destroyed after review by General Counsel.

Additionally, in accordance with NARA Authority N1-311-02-01, Item 4, consumer



records, including community rating system records, are retired to the Federal Record Center (FRC), two (2) years after cutoff and destroyed ten (10) years after cutoff.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that NFIP may maintain information collected longer than is needed or authorized.

Mitigation: This privacy risk is mitigated by only maintaining information within NFIP ITS in accordance with the NARA authority outlined in Section 5.1 of this PIA.

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.

NFIP shares NFIP ITS data with participating federal, state, and local officials as well as the DSA and WYOs involved in floodplain management to increase understanding of flood risks and to encourage them to take actions to mitigate those risks.

Information that FEMA may share externally is accessible to NFIP stakeholders via the BureauNet and Data Exchange.

BureauNet allows access to NFIP general information, manuals, and TRRP static reports based on requestor's access privileges/permissions. Certain web pages within BureauNet require a user name and password. Requests for access to these restricted/secured BureauNet web pages are submitted to, and only authorized by, the NFIP ITS Program Manager, COTR, and System Owner. Once approvals have been granted by the NFIP ITS Program Manager, COTR, and System Owner, a user account and password will be generated for the user to login to the restricted/secured areas under BureauNet.

Data Exchange allows the DSA and WYO companies, contractors, and State Coordinators to query "real-time" TRRP data to the NFIP ITS mainframe. Level of access granted is dependent on the user type. For example, the State Coordinator from Mississippi can only see data for that state. Also, the DSA or WYO will only have access to its company data. Requests for access to Data Exchange are submitted to and authorized by the NFIP ITS Program Manager, COTR, and System Owner. Once approvals have been granted, a user account and password will be generated for the user to login.

NFIP ITS provides non-renewed policy information electronically to NFIP's marketing contractor. This information includes, but is not limited to, insured property address, insured name, and WYO Company and policy numbers.



NFIP ITS provides the F&WS with information including the DSA and WYOs and policy numbers, insured's name, insured's property address, date of construction or substantial improvement, and the insured property plat map. The F&WS provides NFIP ITS with a written letter explaining the determination of the property's proximity to the CBRS area, whether it is located within or outside the CBRS area boundary, and the CBRS area effective date. The F&WS may share information provided by NFIP ITS with a GIS mapping contractor for the purpose of processing determinations. This sharing of information between NFIP and F&WS is pursuant to an interagency agreement between the two organizations.

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

Routine use H, as identified within the DHS/FEMA 003 – National Flood Insurance Program Files System of Records, 73 Fed. Reg. 77747, December 19, 2008, allows NFIP to share information with stakeholders including federal, state, and local officials as well as the DSA and WYOs involved in floodplain management to help them understand flood risks and to take actions to mitigate those risks. This is compatible with the purpose for original collection, which includes the administration of flood insurance, and coordination of flood plain management with state and local governments.

Routine use F allows NFIP to share policy information with the F&WS. This is compatible with the purpose for original collection because NFIP requires information regarding the CBRS for flood insurance eligibility in compliance with federal statute.

Routine use F allows NFIP to share policy information with its marketing contractor. This is compatible with the purpose for original collection of information because NFIP uses the information to market the NFIP program to property owners and renters who do not have flood insurance.

6.3 Does the project place limitations on re-dissemination?

NFIP only shares NFIP ITS data with participating federal, state, and local officials as well as the DSA and WYOs involved in floodplain management to help them understand flood risks and to take actions to mitigate those risks. Information provided to WYOs belongs to the WYOs and is subject to the WYO's privacy policies and the state's and local government's privacy regulations. Dissemination of information collected by the DSA on behalf of NFIP is governed by the applicable SORN mentioned in Section 1.2. Additionally, re-dissemination of information collected and maintained within the NFIP ITS is limited by providing the user with a warning banner that informs NFIP ITS users that re-dissemination of NFIP ITS data is prohibited.



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

NFIP maintains audit logs of access of information within BureauNet and Data Exchange. Additionally, as identified in the DHS/FEMA 003 – National Flood Insurance Program Files System of Records, 73 Fed. Reg. 77747, December 19, 2008, requests for NFIP program information are made through the FEMA Disclosure Office which maintains the accounting of records disclosure under the Privacy Act.

NFIP also maintains records of the aforementioned property loss history reports provided to its policy holders.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that information maintained in NFIP ITS may be inadvertently disclosed to entities that are not compatible to the purpose in which NFIP collects and maintains the information.

Mitigation: NFIP mitigates this risk ensuring that sharing of information is consistent with the routine uses outlined in Section 1.2 and all requests and disclosures of information under the Privacy Act are recorded.

Section 7.0 Redress

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

Individuals seeking access to records contained within NFIP ITS may submit a request, in writing, to: FEMA Disclosure Officer, Records Management Division, 500 C Street, SW, Washington, DC 20472. Requests should be clearly marked “Privacy Act Request.” In accordance with 6 CFR § 5.21, the name of the requester, the nature of the record sought, and the required verification of identity must be clearly indicated.

Policyholders will also receive access to their records when NFIP sends them their property loss history. This includes claim and payment information regarding the property (both during and prior to their ownership/tenancy of the insured property).

Additionally, the DSA and WYOs provide procedures and instructions to policyholders on how to correct information on their policies.



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

Individuals seeking to amend their records contained within NFIP ITS may submit a request, in writing, to: FEMA Disclosure Officer, Records Management Division, 500 C Street, SW, Washington, DC 20472. Requests should be clearly marked “Privacy Act Amendment Request.” In accordance with 6 CFR § 5.21 the name of the requester, the nature of the record amended, and the required verification of identity must be clearly indicated.

Additionally, the DSA and WYOs provide procedures and instructions to policyholders on how to correct information on their policies.

Often, NFIP ITS identifies errors in company data, and the companies correct the data in the following month’s reporting cycle.

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

This PIA and the SORNs listed in Section 1.2 provide notice of access and correction. Additionally, the DSA and WYOs provide procedures and instructions to policyholders on how to correct information on their policies. Additionally, there is a formal claims appeals process conducted or monitored by FEMA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that the DSA or WYOs will submit inaccurate information that impacts an individual’s claim.

Mitigation: This privacy risk is mitigated by NFIP requiring use of standard forms by the DSA and WYOs to collection information from property owners and renters. These forms (listed at Appendix A) are approved by the Office of Management and Budget and FEMA’s Records Management Division. In the event of human error, policyholders may request access to their records using the procedures mentions in Section 7.2 and then resubmitting corrected information. Additionally, notice is provided in the SORNs listed in Section 1.2 for procedures to request and resubmit claims appeal information.

Privacy Risk: There is a privacy risk that policyholders will not know how to access and correct their information that is maintained within the NFIP ITS.

Mitigation: This privacy risk is mitigated by NFIP providing notice through this PIA, the SORNs listed in Section 1.2, and the Privacy Act Statement on FEMA forms that reference applicable SORNs, on how to access and correct their information. Additionally, the DSA and WYOs provide procedures and instructions to policyholders on how to correct information on their policies.



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?

There are several levels of access and a broad range of stakeholders who are authorized to view NFIP data. The NFIP ITS Security Plan provides details about the users who are authorized access at specific levels including NFIP and NFIP ITS staff, other federal, state, and local officials, the DSA, and WYOs. The NFIP security authorization process evaluates access levels, user roles, and associated security controls.

All NFIP users, including contractors, have access to national NFIP data sets with view-only capability. NFIP employees and contractors may only update reference data used to verify transactions, such as flood map data used to determine the flood risk of a particular location. State and local users are limited to viewing insurance data within their state or locality. The DSA and WYOs are limited to viewing only their specific company's data, and they are limited to viewing data of the DSA and WYOs policyholders they serve.

Formal procedures are in place for establishing user accounts. For FEMA Wide Area Network (WAN) applications, NFIP approves and verifies all user accounts and assigns access roles using the NFIP data access application process. NFIP ITS security entities verify the identities of users before granting access to the system. A supervisor state official or, WYO will identify a point of contact and request that the user communicate with that contact to obtain access to NFIP. Once the verification process is complete the user receives an initial ID and password based on his or her organization, position, and role. At the end of this process, users receive access authorization. The NFIP program maintains audit records for the system that are sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected.

In summary, NFIP system administrators will have the highest access level; at the lowest level, the DSA and WYOs will be able to view only their company's data.

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

NFIP employees and contractors are required to take initial and annual security and privacy awareness training and acknowledge the Rules of Behavior for personnel assigned to the NFIP ITS before being granted access.



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

Individuals receive access approval through the NFIP account management process. External users submit access requests to NFIP for approval, after which the request is acted upon by the NFIP ITS account management staff. Once the user is verified against the NFIP domain address solution, the account credentials are provided via a secure distribution process. Any verification discrepancies noted and acted on by NFIP management. External users' access to the system is limited to the established NFIP BureauNet public domain website. However, some of the links on this site are protected and require authentication credentials that are established via the access request process through NFIP.

NFIP ITS contractors (internal users) obtain user accounts through the NFIP ITS account management process. Establishing, activating, modifying, disabling, and removing accounts procedures are documented, implemented, and managed by the NFIP Information Technology Division. NFIP user account request forms are used to establish what access is required by the user's supervisor and then approved by NFIP management. All users are assigned individual accounts based on role assignment. If a user within a role requires additional access, it must be specifically requested for and approved. Group memberships are not allowed as an account option. Guest/anonymous accounts are not used, and temporary accounts are established when necessary for authorized users who require short term access, typically less than 24 hours.

Notification of user account changes due to user termination, transfer, or access level needs are communicated to the NFIP Information Technology Division by the user's manager as part of the account management procedures. Temporary accounts are terminated immediately by the Network Operations Manager, who is notified by the System Administrator, after the short term access needs are completed

Privileged users who require and are approved for remote access use the approved Nortel VPN solution using IPSec encryption. External devices used for remote access are not used for storing personal information, and the hard drives are encrypted as standard baseline configuration.



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 review and approval of information sharing agreements, MOUs, Interagency Agreements (IAA), or other sharing of NFIP ITS information must be approved by NFIP ITS Program Manager, COTR, System Owner, FEMA Privacy Officer, and Office of Chief Counsel.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

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



Appendix A - OMB Collection & FEMA Forms Associations

| OMB Collection # | OMB Collection Title | FEMA Form #/Title |
|-------------------|---|--|
| OMB No. 1660-0005 | National Flood Insurance Program Claims Forms | <ul style="list-style-type: none"> • FEMA Form 086-0-6 (formerly 81-40) National Flood Insurance Program Worksheet-Contents-Personal Property • FEMA Form 086-0-7 (formerly 81-41) Worksheet Building • FEMA Form 086-0-8 (formerly 81-41A) Worksheet Building (Continued) • FEMA Form 086-0-9 (formerly 81-42) Proof of Loss • FEMA Form 086-0-10 (formerly 81-42A) Increased Cost of Compliance Proof of Loss • FEMA Form 086-0-11 (formerly 81-43) Notice of Loss • FEMA Form 086-0-12 (formerly 81-44) Statement as to Full Cost of Repair or Replacement under the Replacement Cost Coverage, Subject to the Terms and Conditions of this Policy • FEMA Form 086-0-13 (formerly 81-57) National Flood Insurance Program Preliminary Report • FEMA Form 086-0-14 (formerly 81-58) National Flood Insurance Program Final Report • FEMA Form 086-0-15 (formerly 81-59) National Flood Insurance Program Narrative Report • FEMA Form 086-0-16 (formerly 81-63) Cause of Loss and Subrogation Report • FEMA Form 086-0-17 (formerly 81-96) Manufactured (Mobile) Home/Travel Trailer Worksheet • FEMA Form 086-0-18 (formerly 81-96A) Manufactured (Mobile) Home/Travel Trailer Worksheet (Continued) • FEMA Form 086-0-19 (formerly 81-98) Increased Cost of Compliance (ICC) Adjuster Report • FEMA Form 086-0-20 (formerly 81-109) Adjuster Preliminary Damage Assessment • FEMA Form 086-0-21 (formerly 81-110) Adjuster Certification Application |



| OMB Collection # | OMB Collection Title | FEMA Form #/Title |
|-------------------|--|---|
| OMB No. 1660-0006 | National Flood Insurance Program Policy Forms | <ul style="list-style-type: none">• FEMA Form 086-0-1, Flood Insurance Application• FEMA Form 086-0-2, Flood Insurance Cancellation/Nullification Request Form• FEMA Form 086-0-3, Flood Insurance General Change Endorsement• FEMA Form 086-0-5, Flood Insurance Preferred Risk Policy Application• FEMA Form 086-0-4, V-Zone Risk Factor Rating Form and Instructions |
| OMB No. 1660-0020 | Write Your Own (WYO) Program | <ul style="list-style-type: none">• FEMA Form 129-1, National Flood Insurance Program's Transaction Record Reporting and Processing (TRRP) Plan |
| OMB No. 1660-0095 | National Flood Insurance Claims Appeal Process | <ul style="list-style-type: none">• No Forms |