
# Privacy Impact Assessment
for the

# National Flood Insurance Program (NFIP) Modernization /Business Process Improvement/Systems Engineering Management Support

# (NFIP Information Technology Systems/NextGen)

November 26, 2008

**Contact Point**
Jack Way
Mitigation Division, Risk Insurance Operations
Federal Emergency Management Agency
(703) 605–0750

**Reviewing Official**
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

## Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency's (FEMA) National Flood Insurance Program (NFIP) Modernization, Business Process Improvement, and Systems Engineering Management Support project has transitioned into NFIP IT (NextGen). The NFIP IT NextGen service oriented and integrated systems will support daily reporting by NFIP insurance companies and improve services to stakeholders, especially policy holders. The purpose of this PIA is to describe the collection of information in conducting NFIP processes and how NFIP information is used by FEMA and the NFIP community.

## Overview

In 1968, Congress created the National Flood Insurance Program (NFIP) in response to the rising cost of taxpayer funded disaster relief for flood victims and the increasing amount of damage caused by floods. The Mitigation Division, a component of FEMA, manages the NFIP and oversees *the floodplain* management and mapping components of the Program.

Nearly 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. In exchange, the NFIP makes federally backed flood insurance available to homeowners, renters, and business owners in these communities.

FEMA established a system of records under the authority created by the Flood Insurance Act of 1968 as amended, 42 U.S.C. § 4100, *et seq.* Currently the aging FEMA NFIP architecture restricts access to data, takes months to update, and limits automated options to make NFIP data more accurate authority. For these reasons, the FEMA NextGen effort is focused on improving NFIP existing processes with proven, secure and up-to-date technologies.

Typically, a home or business owner will seek flood insurance from an insurance company that provides other lines of business such as traditional car insurance or property and casualty homeowners insurance. In other cases, a mortgage lender will require flood insurance in addition to regular homeowner's insurance. If a home owner's insurance company participates in the NFIP's Write-Your-Own (WYO) program, and the home or business owner's building is located in a participating NFIP community, the home or business owner can purchase flood insurance.

By law, there is a 30-day waiting period prior to a policy becoming effective, however, under the current reporting process, WYO insurance companies do not receive validation from FEMA until as many as 60 days following a policy issue or claim submission. WYO insurance companies and their policy holders are unsure of their status due to antiquated systems employed by FEMA, resulting in processing delays to their policy or claims information. In the past this monthly system cycle was adequate because the insurance business operations were not as fast paced nor were the economic impacts as high. Increased real estate development and recent severe hurricane seasons clearly establish the need to accelerate FEMA's validation processes and its ability to more closely scrutinize NFIP insurance companies' activities. The current FEMA NFIP systems architecture dates back to the 1980s and will soon become unsustainable.

FEMA's NextGen project is a 5 year reengineering/re-hosting effort that began in FY 2003. Its primary goal is to replace the existing technologies of the current existing FEMA Privacy Act system of records, the "National Flood Insurance Bureau and Statistical Agent (BSA) Data Elements and Related Files", FEMA/FIMA-3, 67 FR 3191 (January 23, 2002). The existing System of Records Notice (SORN) will be updated in conjunction with this PIA.

In January 2008, the NextGen project began its transition to the NFIP IT which operates and maintains the new technological infrastructure. NFIP IT will not require the collection of any additional personally

identifiable information (PII) from individuals beyond what FEMA has described in the updated SORN. Rather, NextGen – NFIP IT is an update of the electronic architecture planned to go into effect during CY 2008 that will enable FEMA to collect and report NFIP information in a more efficient way.

Specifically, FEMA collects PII only for the purposes of verifying the accuracy of NFIP flood insurance policies and claims, to prevent fraudulent claims, and for the oversight and management of the NFIP rather than to directly deal with insured individuals. FEMA NextGen has addressed the major areas relevant to this privacy impact assessment.

FEMA's NFIP NextGen consists of technologies that will 1) accelerate updates by increasing access to authorized personnel via the World Wide Web; 2) develop a rules engine that identifies possible errors before flood insurance policies go into effect; 3) effectively track NFIP policy and claims data to facilitate corrections; and 4) provide FEMA policy makers with the capability to assess NFIP's program-wide status on the soundness of business operations. Once FEMA NextGen prototypes are fully tested and piloted, they will be implemented, with accompanying plans and policies in regular NFIP operations. The primary NextGen Modules that will be fully operational in 2008 are briefly described below.

- **The Transaction Record and Reporting Process (TRRP):** TRRP will collect and report transaction data from WYO insurance companies on a daily basis in NextGen. This is an upgrade from the current process that collects information on a monthly basis. This is one of two mandatory processes for WYO insurance companies participating in the NFIP. The TRRP is the primary means by which WYO Insurance Companies receive validation that they are performing NFIP flood insurance transactions properly.

- **Flood Financial Management (F2M):** In conjunction with their mandatory TRRP submissions, WYO insurance companies, or a vendor on behalf of a NFIP WYO insurance company (i.e., the participating insurance company), must submit financial data such as the amount of the claim and the premium that accompanies the transactions a WYO insurance company or vendor carried out, such as premium collected or claims payments, as expected in performing NFIP business and reported in their daily TRRP submission. No PII related to a particular payment is provided, only the amount attributed to a specific transaction.

- **The Flood Rating Engine Environment (FREE):** An online tool for WYO insurance companies and vendors to use to accurately develop insurance policy quotes. A quote requires only the location and description of a structure. Other than the address, no PII is included within a quote. WYO insurance companies and vendors must apply for a username and password to use this tool.

- **ezClaims:** NextGen ezClaims provides a one-stop shop application for NFIP stakeholders such as certified flood claims adjusters, FEMA claims analysts and claims managers to input, view, validate, and manage NFIP insurance claims, disaster information, re-inspections and flood certified adjuster data. ezClaims is comprised of six modules, that are available to authorized and authenticated users based upon a verified business need and role. Each module provides access to specific business-driven features designed to facilitate reporting, monitoring, and workflow management of NFIP claims-related information. The modules include:

    - Company Claims - A temporary module in place that collects WYO claims data on a weekly basis until the Daily TRRP takes effect as planned for 8/11/2008.

    - Re-inspection - Manages the assignment of certified flood adjusters and what data the adjuster must collect as part of FEMA's reinspections of claims.

    - Disaster Information – Supports the assignment of Flood Insurance Claims Office (FICO) numbers to large flooding events indicating the impacted states and counties to help monitor claims activities.

- Coordinating Office - Supports the coordination of wind and flood insurance claims with coastal States.
- Damage Assessment – Supports online preliminary damage estimates entered by certified flood adjusters in the field.
- Adjuster Console - Supports tracking and maintenance of certified flood adjusters continuing education credits.

WYO companies and vendors must apply for a username and password to gain access to this tool.

- **Simple and Quick Access Net (SQANet):** SQANet is the consolidated reporting tool for authorized and authenticated NFIP stakeholders (stakeholders include FEMA, WYO Companies and State employees) that analyze NFIP data, and provide aggregate reports about NFIP activity. For example, this reporting tool is used to report policy growth across the U.S., report claims activities, to look up specific policies or claims or any other number of program analysis, oversight or inquiry activities. When reviewing specific policy or claims information, authorized users can view homeowner names, addresses, premiums, rating characteristics and claims information related to structures covered by the NFIP.

The core NFIP NextGen technologies described above will become the main support toolset for FEMA's oversight, guidance, and communications with WYO insurance companies. These web-based tools will enable FEMA to more efficiently direct NFIP business transactions and then expedite responses to NFIP claims when policy holders require urgent support. All of these tools are accessed from the NFIP IT Services Web portal www.nfipbureau.fema.gov where stakeholders can learn additional information about NFIP IT, what was formerly the NextGen project, and apply to receive authorized access to NextGen tools under the request access link under My Profile. Not everyone is authorized for access, only those who are authorized by their employers and FEMA NFIP IT security.

The objective of the PIA is to assist the DHS/FEMA staff to identify and address privacy requirements when planning, developing, implementing, and operating individual agency information management systems. The PIA process also helps to identify sensitive systems so that appropriate information assurance measures are in place.

This privacy impact assessment is being conducted in order to outline the NFIP program and how the NextGen Modernization effort affects the information collected and used in the NFIP.

# Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

## 1.1 What information is collected, used, disseminated, or maintained in the system?

Information contained in the NFIP can be grouped in two major categories:

- Individual Insured Information:
  - Individual's Information: Full Name, property address insured, and home mailing address of individuals who apply for flood insurance is passed onto FEMA for verification that the location may be covered by NFIP.

- Claims Information: Subsets of claims files are collected to monitor the WYO companies' claims processes to verify that policy holders received proper services and payments.
- Building and Contents Information: includes data regarding the location of a building or an individual's residence, its construction and how it relates to flood risks. An example of building information might include an individual's home street address, flood risk zone and participating flood community. Contents information typically describes machinery, equipment and other items inside individual homes or businesses that could be damaged by flooding. FEMA uses this information is used to analyze and evaluate the financial risks assumed by the NFIP, to determine sound rules and rates, to monitor WYO transactions and to support recovery efforts.
- Payment Information: FEMA does not collect this information. Information used to verify payment information, such as cancelled checks for premiums or claims, remains with WYO companies. As of May 1, 2008 all NFIP insurance forms and processes will no longer collect social security numbers (SSNs). All NFIP IT systems have removed all SSN data to reduce the severity of any breach of privacy. Any SSNs that were collected have been expunged from legacy systems. FEMA audits have ensured SSNs are not in NFIP systems.

- Users of NFIP: For NFIP IT Systems, user accounts are based on unique and official email addresses. WYO users who required access to NFIP IT systems are validated through their respective Companies' flood insurance director and provide only name, email address, work phone number and company information to receive authorization by FEMA to access only their company's data. The first validation of an access request is performed by a known point of contact (POC) within a WYO Insurance Company or State NFIP Coordinator's office. The information requires the previously mentioned email address and current phone number. The business address is used for the requester's location. The direct supervisor and known POC verifies the specific need required by a requester. The overall process is summarized below.
  - The Request & Approval Process requires the following steps
    - 1. Requests Access (normally the end user)
    - 2. NFIP IT Security Defines Access Level
    - 3. Gain Approval from WYO Company/Vendor POC
    - 4. Gain Approval from FEMA ISSO POC
    - 5. Communicate Results to Requester

## 1.2 What are the sources of the information in the system?

The information is provided to the NFIP from participating WYO insurance companies. WYO insurance companies use licensed insurance agents to collect NFIP policy information from individuals and submit accepted quotes to their respective companies.

WYO insurance companies formally agree to participate in the NFIP. Part of the "Arrangement" requires the WYO insurance companies to report on NFIP related transactions via the TRRP. The TRRP process was established in 1983 with the initiation of the WYO program to support FEMA's oversight of WYO activities. Licensed insurance agents and adjusters provide policy and claims data respectively to their respective WYO companies, which then pass the required TRRP summary data to FEMA. Citizens willingly provide their personal information in the same manner as they would with any other business transaction with a chosen insurance company. FEMA's focus is on the structure at a particular location; much of a citizen's PII is not important to FEMA's oversight of policy underwriting and claims adjusting activities.

Insurance companies provide summary of their claims and underwriting processes, minimizing the amount of PII passed to FEMA. NFIP participating insurance companies recognize their responsibility to maintain accurate information as part of the formal arrangement.

WYO users who required access to NFIP IT systems are validated through their respective Companies' flood insurance director.

## 1.3 Why is the information being collected, used, disseminated, or maintained?

FEMA requires WYO companies to submit TRRP data that may be collected from individuals in order to support NFIP operations oversight. Individual's PII such as name, and home mailing address included in the transaction data helps to verify insurance purchases. Buildings, including individual's homes and their contents information are reported to support proper flood insurance underwriting and claims practices. FEMA is responsible for ensuring the NFIP's financial health and ensuring that program services are consistently provided. FEMA collects PII to verify the accuracy of NFIP flood insurance policies and claims, to prevent fraud, and to oversee the NFIP process. In addition, the NFIP is responsible for making certain the NFIP transaction records in conjunction with WYO insurance companies' financial reports supports verification and validation of proper program execution. This reporting operation supports FEMA's knowledge of program activities performed by insurance companies and that citizens received the proper services. The reporting operations also support FEMA's efforts to prevent fraud and abuse within the NFIP.

## 1.4 How is the information collected?

Initial policy and claims information may be collected in the field through handwritten forms completed by a customer and agent, however most companies utilize information systems to collect the information required for sound insurance practices. The WYOs then consolidate their transactions for a given day and submit their data to FEMA via the encrypted TRRP submissions.

During the purchasing process a home or business owner will work with a certified NFIP insurance agent to gather detailed information required to complete the NFIP Flood Insurance Application (OMB No. 1660-0006). Assuming the information is correct and the property is eligible for NFIP insurance, the agent's WYO insurance company will issue the policy and report a subset of the information contained in the application to FEMA for validation.

## 1.5 How will the information be checked for accuracy?

The NFIP Bureau and Statistical Agent compiles all of the WYO companies' data and reports it to FEMA NFIP administrators to perform manual validation reviews, in addition to the automated TRRP process previously mentioned. Additionally, FEMA executes periodic underwriting audits and claims re-inspections to check for operational accuracy at the insurance companies. Because FEMA's focus is on underwriting and claims processes, the data used to examine the structure and its location is the primary link to a citizen that is reviewed for accuracy. Insurance companies are responsible for the accuracy of any financial transactions with their customers who may be U.S. citizens. Over the long term, citizen links to structures and locations can change many times, so it is more important that FEMA understands the risk of a structure at a particular location than the individual. The primary responsibility for checking the accuracy of individual NFIP customers lies with the insurance companies. Insurance companies will often perform credit checks and require identification as part of their normal business processes.

NextGen/NFIP IT technologies will enter production operations in 2008 to conduct data validation processes earlier to help reduce error prone data elements such as building addresses, which continue to focus on a structure and its location.

FEMA is helping to improve policy and subsequent claims data accuracy by automatically providing WYO companies accurate rating, flood zone, community and other pertinent data as soon as possible in policy and claims processes to support optimal policy holder services. The NFIP Flood Manual that is updated twice annually is the primary source for how the transactions are to be conducted by WYO insurance companies and serves at the basis for automated services.

Additionally, NFIP NextGen/NFIP IT systems utilize commercial geo-coding data and United States Postal Service address data to help validate structure locations and addresses, "Reference Data". This "Reference" data purchased by FEMA is also used to verify and validate the NFIP business transaction carried out by WYO insurance companies as previously discussed. FEMA utilizes data from the USPS, Local Governments, and by industry standard geo datum verified by national bodies such as the U.S. Geological Survey.

### 1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Flood Insurance Act of 1968 as amended, 42 U.S.C. § 4100, *et seq* establishes the legal authority of the NFIP. The WYO program under the National Flood Insurance Act established the annual Agreement by which every WYO company complies. By May 2008 all companies and vendors participating in the TRRP process will complete Interconnection Security Agreements to further ensure systems security compliance across the Program.

### 1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy risks are mitigated for FEMA NFIP NextGen technologies by only requesting basic PII from WYO companies to verify and validate transactions. By focusing on structures and their locations, FEMA minimizes the risk of comprising policy holder PII. Overall, annual security and financial audits are conducted to review security controls to further ensure NFIP data is protected and risks are continuously mitigated. Examples of technological security controls in place to mitigate risks to privacy include firewalls, antivirus prevention and detection systems, role based access controls and encrypted communications.

In reviewing the data required, FEMA determined that Social Security Number was no longer required. This has reduced the amount and sensitivity of PII, FEMA maintains.

## Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

### 2.1 Describe all the uses of information.

NFIP participating WYO insurance companies provide summary data that FEMA uses to validate all transactions including, but not limited to policy underwriting, claims authorization and policy renewals; and to help guide and validate flood mitigation efforts. FEMA NextGen prototypes (usable applications released for testing) are under development to support these activities and are scheduled for phased implementation during the 2007 - 2008 calendar years. In the NextGen/NFIP IT systems, PII may be used to answer policy or claims questions, to lookup detailed policy information. Additionally, in cases where FEMA needs to provide specific underwriting or claims direction to a WYO company, PII such as an address

ensures that FEMA and the WYOs are discussing the same specific structure. For example, underwriters and claims examiners will use the address and the corresponding structural information from that address to ensure a policy holder pays the proper premium or the proper claims are paid for flood related damage.

The information provided to FEMA is intended to support oversight that ensures consistent and proper NFIP services for policy holders while avoiding intelligible policies and claims processing. FEMA collects PII to verify the accuracy of NFIP flood insurance policies and claims, to prevent fraud, and to oversee the NFIP process. The SQANet system provides reports to FEMA and other stakeholders for routine research of policies and claims processes and to help mitigate future flooding events, as previously mentioned.

## 2.2 What types of tools are used to analyze data and what type of data may be produced?

NextGen tools, such as SQANet, are used to analyze and verify flood insurance transactions primarily provided via the TRRP and do not generate additional data or previously unavailable *data* regarding individuals. WYO companies can access their TRRP errors and validated data via SQANet to then follow-up on errors or other questions related to any NFIP transaction they performed. FEMA and States review the TRRP data to perform mitigation activities and to review WYO operations.

## 2.3 If the system uses commercial or publicly available data please explain why and how it is used.

NFIP NextGen systems utilize commercial geo-coding data and United States Postal Service address data to help validate structure locations and addresses. This "Reference data" purchased by FEMA is also used to verify and validate the NFIP business transaction carried out by WYO insurance companies as previously discussed. FEMA utilizes data from the USPS, Local Governments, and by industry standard geo datum verified by national bodies such as the U.S. Geological Survey.

## 2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Technical security controls, rules of behavior policies, security awareness communications and other security processes, such as periodic audits and log reviews, work in concert to ensure that information is properly handled throughout the NFIP. For example, all NFIP IT user access applications undergo a multi-layered verification, validation and authorization process. When an individual requests access to NFIP IT systems, their request is first verified by an established authorizer for that level, such as a WYO Company Flood Operations Director. Based on the information provided by an applicant and a Director's verification that the request is valid, the FEMA NFIP IT ISSO reviews the applicant's data verifies that there is a valid need for access for routine use of NFIP data and that the applicant's supervisor has validated the request. At that time the applicant may or may not receive access to NFIP IT systems with the minimal access required to perform their specific business. In all cases, WYO company personnel are only enabled to see their company's data. Likewise, State NFIP Coordinators are only able to view their specific state's data. Within FEMA, personnel are limited to access data commensurate with their position responsibilities. Overall, role-based access, usernames, passwords, security awareness programs that address rules of behavior, and monitoring/auditing technologies are included in NextGen systems architectures and ongoing plans. Intrusion detection capabilities are also required for FEMA NextGen systems to prevent unauthorized access to NFIP databases. See sections 4 and 8 of this document for detailed usage and technical security controls information.

# Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

## 3.1 How long is information retained?

In accordance with the Federal records retention requirements and as indicated by the updated Privacy Act NFIP system of records notice, policy records are destroyed 5 years following the termination of a policy (N1-311-86-1,Item 1A13a(2)). Claim records are maintained for 6 years and 3 months after final action, unless litigation exists. Records are disposed of IAW FEMA Records Schedule N1-311-86-1, Item 2A12(2)(b). Claim records with pending litigation are destroyed after review by General Counsel IAW FEMA Records Schedule N1-311-86-1, Item 2A13a(1). Consumer records, including Community Rating System records, are retired to the Federal Record Center 2 years after cutoff, and destroyed 10 years after cutoff, IAW FEMA Records Schedule N1-311-02-01, Item 4.

## 3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. NFIP files are under record group 311 and individual files generated are covered by FEMA File Numbers FIA-1 through FIA-13-3-3. These record retentions have been approved by the NARA (Job Number N1-311-86-1) and are published in FEMA Manual 5400-2M, dated February 2000.

## 3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The NFIP Risk level decreases as policy and claims records that contain PII are archived and taken off-line after one year and then fully expunged after 5 years. PII is not required for actuarial trends analysis or policy and claims experience analysis across the program. When PII is no longer needed, the data is transferred to tape that is degaussed or wiped, preventing any data to be retrieved.

PII risks are minimal due to the lack of SSN/Taxpayer ID information in the systems. Typically this information is not required for the types of analysis related to floodplain and actuarial management. The only time historical claims information is accessed is in the event of additional flooding or at policy renewal. In these cases the historical data is only verified and validated and not necessarily circulated. The historical claims information indicates that flooding had occurred at a specific time and location, involving a particular structure. This data is required to inform future owners of a structure that has a significant risk of flooding and when new owners are purchasing a previously flooded structure, the new policy is rated correctly.

# Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

## 4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The DHS FEMA Mitigation Directorate, Risk Insurance Division is the primary recipient and user of NFIP insurance data.

Other FEMA Mitigation Division groups, such as the Risk Analysis and Risk Reduction Divisions use NFIP data to support floodplain management activities and to support mitigation efforts. For example, FEMA regional personnel use NFIP data to verify claims filed by NFIP policyholders, perform mitigation analysis, and create plans for mitigation projects. At summary levels, aggregate flood claims data is used to identify flooding history and to guide mitigation projects.

## 4.2 How is the information transmitted or disclosed?

NFIP information is transmitted to FEMA via encrypted data files, automatically uploaded by a WYO insurance company server to the NFIP secure FTP server. Individual authorized users may view data online using FEMA issued username and passwords commensurate with their position and role requirements.

## 4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

NFIP data must be shared among internal stakeholders to properly oversee, manage, assist, and most importantly, support NFIP policy holders during flooding disasters. Risks associated with sharing NFIP data are mitigated by frequently reminding users of their responsibilities in maintaining privacy through security training and automated privacy act notices that must be agreed to prior to accessing NFIP reports. Additionally, specific controls as described throughout this document further mitigate unintended sharing of data with unauthorized personnel. Section 2.4 describes how FEMA mitigates unauthorized access risks via its rigorous and compliant access application process, which ensures that FEMA is fully aware of all users who have access and what data they access to perform required activities. All FEMA users, including contractors, have access to national NFIP data sets with view-only limitations. Government personnel and government 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.

# Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

## 5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

As part of their arrangement with FEMA, WYO insurance companies are responsible for controlling access to individual's PII that they collect and control. In order to participate in the NFIP, WYO insurance companies are required to maintain an individual's privacy. FEMA is also responsible to the companies for ensuring that their individual customers' data remains confidential. FEMA signs and the Arrangement and Interconnection Security Agreements (ISA) with WYO insurance companies and vendors to formalize and share information about the various security responsibilities and controls, as described in this document.

FEMA NextGen systems are required to share data with other NFIP stakeholders including *communities*, states and other FEMA organizations that are involved in floodplain management to help them understand flood risks and to take the appropriate actions to mitigate flood risks. For example, in response to flood insurance claims, FEMA often helps state and communities to establish stronger building codes. At a minimum, authorized floodplain management stakeholders will be issued usernames and passwords by FEMA to control access to NFIP data. All authorized users will be tracked and monitored to prevent NFIP data misuse and unauthorized access.

Other FEMA Mitigation Division groups will use NFIP data to support floodplain management activities and to support mitigation efforts. For example, FEMA regional personnel will use NFIP data to verify claims filed by NFIP policyholders. State and community organizations will use the data to prevent fraud and misuse of the NFIP's flood insurance. At summary levels, aggregate flood claims data is used to identify flooding history and to guide mitigation projects.

Each state and community agency is required to provide FEMA its mechanisms (such as a systems security plan) for assuring data and individual's privacy. Until FEMA reviews a state's documentation and is assured that a cooperating agency will properly use NFIP data, then FEMA will make the data accessible on a limited access. (e.g. The town of XXX can only be granted access to floodplain mitigation data for the town of XXX and not to the town of YYY's NFIP data.) The NFIP Information Systems Security Officer (ISSO) is responsible for ensuring DHS standard ISA are honored and enforced by other agencies and NFIP stakeholders. Additionally, the information is shared under the routine uses is already described in the National Flood Insurance Bureau and Statistical Agent's BSA's Data Elements and Related Files" systems of records notice.

FEMA NextGen/NFIP IT is integrating data reporting software products such as Oracle Reports and Business Objects with Computer Associates (CA) security software to provide limited role-based access. The NextGen architecture will complete security certification and accreditation processes to ensure privacy is maintained across agencies. This means that NextGen technologies will be routinely examined and certified that they are able to accurately identify users accessing data, track their activities and prevent them from accessing data they are not authorized to view.

In this way, routine data usage revolving around addresses and structures linked to addresses remains the focal point of ongoing NFIP operations. Over time PII is unnecessary for understanding long term flood risks and conducting strategic mitigation activities to prevent repeated damage from flooding. DHS/FEMA may make disclosures from this system to "consumer reporting agencies" as defined in the Fair Credit Reporting Act 15 U.S.C. 1681a(f), as amended; or the Federal Claims Collection Act of 1966 31 U.S.C. 3701(a)(3), as amended.

### 5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

An ISA/MOU is prepared for all of the various NFIP stakeholder organizations that apply to access NFIP private data. Each ISA/MOU is developed to share information regarding the specific systems and user communities and their roles in NFIP processes. For example there is a standard ISA/MOU for WYO insurance companies, vendors, communities and other DHS/FEMA systems.

### 5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

NFIP Insurance data is shared with mortgage stakeholders via encrypted file exchange for the purpose of complying with federal mandatory flood insurance purchase regulations dating back to the Flood Disaster Protection Act of 1973.

### 5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The primary risk to sharing NFIP data externally is that the use of the data to pursue fraudulent insurance or grants transactions. FEMA mitigates this risk by only retaining name, address, and structural data to ensure PII is not misused during disaster support activities where information is rapidly requested and used to respond to victims needs. FEMA monitors transactions related to insurance claims and grants to prevent fraudulent duplication of benefits as much as possible. Overall, FEMA's primary means of mitigating risks related to PII is by not using the PII as the primary means for tracking policy and claims transactions.

## Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

### 6.1 Was notice provided to the individual prior to collection of information?

This PIA and the updated NFIP IT SORN help to provide the public notice of the information collected as part of normal flood insurance business transactions. NFIP WYO insurance companies routinely inform their policy holders of their privacy guidelines and practices and require policy holders to sign an acknowledgement statement as part of the policy purchase process. Individuals are typically aware of the informational requirements for purchasing insurance. NFIP Flood insurance is very similar to other lines of

insurance and requires the same type of personal data that a consumer would provide for property and casualty insurance. Individuals' NFIP data resides primarily with their WYO insurance company and only a subset is forwarded to FEMA for transaction validation and verification.

To further educate the public about the NFIP and how homeowners can purchase flood insurance and to answer general questions about the NFIP, FEMA has maintained the Floodsmart marketing campaign. This information can be accessed via http://www.floodsmart.gov/floodsmart/

## 6.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals are informed that if they do not provide their requisite personal information, such as their name, address but not their SSN, they cannot purchase flood insurance from the NFIP. The information is required in order to create a proper and binding insurance policy. (NFIP Flood Insurance Application, OMB Form # 1660 – 0006). As of May 1, 2008, SSNs will not be required for purchasing NFIP flood insurance.

## 6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

FEMA receives summary information from insurance companies and does not routinely interact with individuals. An individual's information is used by FEMA only for the purposes of verifying NFIP flood insurance policies and claims accuracy. For example an individual's home address would be used by FEMA to check the accuracy of its floodplain location and risk to ensure that the correct flood insurance premiums are being charged for that specific address. Or such home address may be used by FEMA to identify which community flood mitigation plan applies to that specific property.

## 6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Insurance companies typically provide their policy holders information on their privacy maintenance policies. All NFIP policy holders are aware of the information they provide to their insurance company for the purpose of purchasing NFIP flood insurance. Under the Flood Insurance Reform Act of 2004 (S.2238/P.L. 108-264), Congress requires the NFIP to ensure that its policyholders receive important information about their flood insurance coverage. The law also requires FEMA, to submit an Acknowledgement Form for policy holder signature. This form simply acknowledges that information has been received.

Each policy holder's insurance company provides policyholders with a copy of their flood insurance policy, the Summary of Coverage, and declarations page. The Declarations Page includes the policy limits, as well as the deductible limits and information regarding PII.

# Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Individuals seeking notification and access to any records contained in the system of records, or seeking to contest its content, may inquire in accordance with instructions appearing at 6 CFR Part 5.

Requests for Privacy Act protected information must be made in writing, and clearly marked as a "Privacy Act Request." The name of the requester, the nature of the record sought, and the required verification of identity must be clearly indicated. Requests should be sent to: FEMA Privacy Officer, DHS/FEMA, 500 C Street, SW., Washington, DC 20472.

FEMA NextGen technologies facilitate secure access to data to authorized individuals through CA software products: SiteMinder and IdentityManager. This software supports username and password assignment, administration, maintenance, and auditing. The software supports strong password generation and complies with National Institute of Standards and Technologies (NIST) Special Publication: Guide for the Security Certification and Accreditation of Federal Information Systems (NIST 800-37) and the DHS Sensitive Systems Handbook 4300A.

## 7.2 What are the procedures for correcting inaccurate or erroneous information?

See the Notification Procedure described above.

Typically, individuals work with their respective insurance company to correct erroneous information contained in their policies. Often, FEMA identifies errors in company data, and the companies correct the data in the following month's reporting cycle.

NextGen technologies will increase the opportunities and options for WYO insurance companies to correct erroneous information. For example, addresses are checked for correctness after WYO insurance companies have submitted their transaction information. In FEMA NextGen systems, companies will be able to validate addresses to make sure they are correct by FEMA standards prior to writing a policy.

## 7.3 How are individuals notified of the procedures for correcting their information?

NFIP policy holders are in contact with their NFIP insurance agents and are notified by their agents if their company or if FEMA has identified corrections to their policy or claims information.

NFIP flood insurance agents may communicate with their customers in any way as long as the correction results in an endorsement to flood insurance policy. Endorsements are made to policies to formally make changes to policies as agreed upon by both the policy holder and the WYO insurance company.

### 7.4 If no formal redress is provided, what alternatives are available to the individual?

NFIP WYO insurance companies provide formal redress processes for their NFIP insurance customers. Additionally there is a formal claims appeals process conducted by WYO insurance companies and monitored by FEMA.

(Refer to http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_nfipappeals.pdf)

### 7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

WYO insurance companies typically provide their policy holders information on their privacy maintenance policies. All NFIP policy holders are aware of the information they provide to their insurance company for the purpose of purchasing and processing NFIP flood insurance.

## Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

### 8.1 What procedures are in place to determine which users may access the system and are they documented?

There are several levels of access and a broad range of stakeholders who are authorized to view NFIP data. The FEMA NextGen Security Plan fully details who has authorized access at specific levels within FEMA, WYO insurance companies, and other agencies. The systems security Certification and Accreditation process (to be completed in June 2008 will evaluate each access level, all roles, all processes, and associated security controls.

All FEMA users, including contractors, have access to national NFIP data sets with view-only limitations. Government and government 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 users are limited to viewing insurance data within their state; likewise for community users. WYO insurance company users are limited to seeing only their specific company's data. WYO insurance companies and vendors are limited to viewing data of the WYO insurance companies they serve.

FEMA verifies all user accounts and assigns access roles using the NFIP data access application process. Users who request access to NextGen systems are first verified to confirm their identity through established NFIP entities and appropriate contact information is provided. Once a user's identity is verified, they are provided an ID and initial password based on their organization, position, and role. Access authorization for users is then provided at the end of the process.

FEMA's NFIP IT Services Security Plan includes detailed descriptions of the technology and the organizational personnel responsible for controlling access to NFIP data.

Some users will have limited access based upon their role in the NFIP as described above. FEMA NextGen systems are required to incorporate role-based access to ensure authorized users have permitted access. In summary, FEMA personnel that are designated system administrators will have the highest access level, and at the lowest level, WYO insurance companies will be able to view their and only their company's data.

## 8.2 Will Department contractors have access to the system?

FEMA requires contractor support and provides access to contractors to maintain and update NFIP NextGen systems.

## 8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

FEMA DHS employees and contractors are required to take annual privacy training and acknowledge rules of behavior for all personnel assigned to work with NFIP NextGen systems.

## 8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, FEMA's NextGen security technologies comply with the following relevant DHS, National Institute of Standards and Technologies (NIST), The President's Office of Management and Budget, (OMB) and FEMA security guidance including:

- DHS Sensitive Systems Policy 4300A v5.1;
- FEMA Information Technology Computer Security Incident Management Program (SOP 1540.1-1);
- OMB Management of Federal Information Resources Circular A-130;
- NIST Recommended Security Controls for Federal Information Systems SP 800-53;
- Homeland Security Presidential Directive HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection";
- Federal Information Security Management Act of 2002 (FISMA).

FEMA NextGen purchased CA SiteMinder and IdentityManager products because they comply with FISMA and the additional standards listed above. FEMA is periodically updating NextGen design documentation and configuring the software, so that these security products will ensure compliance with current and future federal electronic regulations.

FEMA NFIP IT Services (NextGen) is currently finalizing security plans and technologies to follow the above referenced security requirements.

FEMA NFIP IT Services (NextGen) includes an annually updated risk assessment as part of its security planning and implementation processes.

FEMA NFIP IT Services (NextGen) includes an annually updated risk assessment as part of its security planning and implementation processes.

FEMA performs annual test plans for NFIP IT (NextGen) security technologies to include documented results to ensure that access to the architecture is secure. FEMA NFIP IT (NextGen) security plans and guides include detailed processes that are compliant with National Institute of Standards and Technologies (NIST) 800-53 security controls such as security assessment plans are maintained properly to safeguard NFIP information.

### 8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Role-based access, usernames, passwords, security awareness programs conducted with all stakeholders at conferences and meetings, (including DHS Rules of Behavior, Annual NFIP IT Security Training) and monitoring/auditing technologies are included in NextGen systems architectures and plans. Intrusion detection capabilities are also required for FEMA NextGen systems to prevent unauthorized access to NFIP databases.

FEMA monitors an individual's use of NextGen modules using CA SiteMinder and IdentityManager software. Authorized users that agree to abide by Federal Privacy Law are monitored via logs that track which reports they access or what other functions they perform per session. Logs are periodically reviewed and audited to identify misuse. Alarms are in place as part of an intrusion detection system that includes auditing capabilities to support preventing unauthorized use and documenting cases where unauthorized use might have occurred.

FEMA NFIP IT (NextGen) systems are for authorized usage only and users agree to terms that include monitoring of their activities. FEMA will utilize the same controls included in CA security software such as audit reports and user session reports to account for usage monitoring policies.

### 8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Technical and manual processes make up over 150 documented security controls to mitigate risks to privacy. By establishing user access controls, physical and virtual access barrier, and conducting regular security and privacy awareness campaigns FEMA is vigilant in protecting NFIP policy holders' privacy.

## Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

### 9.1 What type of project is the program or system?

FEMA NextGen is currently operating under the existing FEMA Privacy Act system of records, FEMA/FIA-3 the "National Flood Insurance Bureau and Statistical Agent (BSA) Data Elements and Related Files 67 FR 3191 (January 23, 2002). This notice will be updated in conjunction with this PIA.

No. In November, 2003 the FEMA determined that Netegrity SiteMinder and IdentityManager security software (now owned by CA) products would meet Federal computer and electronic security requirements for the NextGen project.

A primary objective of the technology is to secure NFIP information while ensuring its confidentiality, integrity and availability. Securing the information protects against possible data breaches, which is the primary privacy risk in regard to the NFIP NextGen program. On a policy level the program has been designed to collect, use, and share the minimum amount of information necessary to complete the mission of the NFIP. On a technological level the system itself and the NextGen modernization effort are directed at ensuring the security of information. Together these two approaches ensure that privacy is considering

regularly during system reviews and policy updates. This PIA will be updated should any changes affecting the substance of the program occur.

### 9.2 What stage of development is the system in and what project development lifecycle was used?

NextGen technologies are in the final stages of development and will go into parallel production with NFIP legacy systems in November 2007. In January 2008, NextGen technologies will initiate transition to become the primary NFIP insurance support systems. NextGen systems began development in FY 2003 following the Boehm spiral development lifecycle that repeatedly reviews requirements and tests the system at various stages, mitigating risks that emerge under other development approaches such as the "waterfall" and "big bang."

### 9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

NextGen systems do not employ technologies that raise privacy concerns.

## Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security