INFORMATION SHARING ACCESS AGREEMENT (ISAA)

BETWEEN

THE DEPARTMENT OF HOMELAND SECURITY/ FEDERAL EMERGENCY MANAGEMENT AGENCY (DHS/FEMA) FEDERAL INSURANCE AND MITIGATION ADMINISTRATION (FIMA)

AND

[LONG NAME OF ENTITY]

1. **INTRODUCTION AND PURPOSE.** The U.S. Department of Homeland Security/Federal Emergency Management Agency, Federal Insurance and Mitigation Administration (DHS/FEMA/FIMA) and [ENTITY LONG NAME (ENTITY SHORT NAME)] voluntarily enter into this Information Sharing Access Agreement (ISAA). The purpose of the ISAA is to enable FEMA to share personally identifiable information (PII) that is protected by the Privacy Act of 1974 (Privacy Act), as amended, 5 U.S.C. § 552a, with the [ENTITY SHORT NAME] to review National Flood Insurance Program (NFIP) policy and/or claims information for [STATE THE SPECIFIC PURPOSE AND USE OF THE NFIP DATA].

2. **AUTHORITIES.** This ISAA is authorized by:

   a. Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 93-288 (1974) (42 U.S.C. 5121 et seq.) (Stafford Act) *for declared disasters only*;

   b. Homeland Security Act of 2002, Pub. L. No. 107-296 (2002) (6 U.S.C. 101 et seq.) *for declared disasters only*;

   c. National Flood Insurance Act of 1968, Pub. L. No. 90-448, Title XIII (1968) (42 U.S.C. 4001 et seq.) (NFIA);

   d. Privacy Act of 1974 (5 U.S.C. 552a) (Privacy Act);

   e. Authority notification - DHS/FEMA 003 –NFIP Files System of Records, 79 FR 28747 (May 19, 2014) (NFIP Files SORN).

3. **BACKGROUND**

   a. [REMOVE THIS PARAGRAPH IF THIS ISAA IS NOT FOR A DECLARED DISASTER] The President declared Major Disasters under the Stafford Act for the state of [STATE NAME] on [DATE OF DECLARATION], as a result of

~~Hurricane~~ XXXX ~~(see~~ PROVIDE FEDERAL REGISTER ~~DOCUMENT CITATION~~).

> NOTE: One community referenced Super Storm Sandy in their ISAA and were then denied current policy information as IAPB refused release of the data as "Current policies in force do not fall under the coverage of the cited ISAA. The city of _____ will need to submit a separate ISAA that covers the needs for this data."

b. FEMA collects, maintains, uses, and disseminates, personally identifiable information (PII) from NFIP policyholders. NFIP policyholder PII is protected by the Privacy Act and shared pursuant to the NFIP Files SORN.

c. As authorized by the routine use provision of the Privacy Act, 5 U.S.C. § 552a(b)(3), FEMA may disclose policyholder PII to federal, state, local, and tribal government agencies to enable them to receive only the NFIP policy and claims information necessary to satisfy a specific routine use as valid and eligible under the NFIP Files SORN.

d. This ISAA encompasses NFIP Files SORN Routine Uses (I), (L), (M), (N), (O), (R), and (T) only.

e. This ISAA encompasses NFIP Files SORN Routine Use (G) for floodplain management enforcement *only*. Any other routine use (G) that involves investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order requires a separate ISAA that must be reviewed and cleared by the FEMA Privacy Office.

f. The [ENTITY SHORT NAME] certifies that it will review NFIP policy and claims information for properties within its jurisdiction [CITE ROUTINE USE DESCRIPTION].

4. **DEFINITIONS.**

As used in this Agreement, the following terms will have the following meanings:

a. COMPUTER MATCHING: Any computerized comparison of two or more automated systems of records, or a system of records with non-federal records, for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs. *See* 5 U.S.C. § 552a(a)(8). Pursuant to 5 U.S.C. § 552a(o), any record contained in a system of records may only be disclosed to a recipient agency or non-federal agency for use in a computer matching program pursuant to a Computer Matching

Agreement (CMA) between the source agency and the recipient agency or non-federal agency.

b. NIST CYBERSECURITY FRAMEWORK: National Institutes of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity," which sets out a repeatable process of, "Identify, Protect, Detect, Respond and Recover," to guide organizational cybersecurity activities and consideration of cybersecurity risk in organizational risk management processes.

c. PERSONALLY IDENTIFIABLE INFORMATION (PII): Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual. For example, when linked or linkable to an individual, such information includes an address, name, social security number, date and place of birth, mother's maiden name, account number, license number, vehicle identifier number, license plate number, device identifier or serial number, internet protocol address, biometric identifier (e.g., photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, and information created specifically to identify or authenticate an individual (e.g., a random generated number). PII constitutes "Controlled Unclassified Information."

d. PRIVACY INCIDENT. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than the authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which raises a reasonable risk of harm.

e. SYSTEM SECURITY PLAN. Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. For instance, technical controls typically include Access Control (IA), Audit and Accountability (AU), Identification and Authentication (IA), and System and Communications (SC).

5. **RESPONSIBILITIES.**

a. FEMA's responsibilities under this ISAA are as follows:

   i. Share with the [ENTITY SHORT NAME] the NFIP policyholder data found in Appendix A of this agreement.

   ii. Transmit the NFIP policyholder data and related information listed in Appendix A to the [ENTITY SHORT NAME] in password protected format via encrypted email.

iii.   Ensure that NFIP policyholder data is accurate, complete, and up-to-date as reasonably necessary.

iv.   FEMA shall not take any adverse action or limit any of its Federal benefits as a result of this sharing of information.

b.   The [ENTITY SHORT NAME]'s responsibilities under this ISAA are as follows:

i.   Use and maintain the NFIP policyholder PII under this ISAA only to review NFIP policy and claims information for properties within its jurisdiction. The NFIP policyholder PII provided by FEMA under this ISAA may not be used for any other purpose.

ii.   Instruct all individuals with access to NFIP policyholder PII regarding the confidential nature of the information, the safeguard requirements of this Agreement, and the criminal penalties and civil remedies specified in federal and state laws against unauthorized disclosure of NFIP policyholder PII covered by this Agreement.

iii.   Employ appropriate administrative, technical, and/or physical safeguards to secure any and all NFIP policyholder PII shared under the provisions of this ISAA, whether in physical or electronic form, and store PII only in places and in a manner, that are safe from access by unauthorized persons or for unauthorized use.

iv.   Limit access to NFIP policyholder PII provided by FEMA under this ISAA only to the authorized [ENTITY SHORT NAME] personnel to review NFIP policy and claims information for properties within its jurisdiction on behalf of [ENTITY SHORT NAME]. This includes all entities and individuals listed in paragraphs 6 and 7.

v.   The [ENTITY SHORT NAME] will not further disclose NFIP policyholder PII provided by FEMA to outside third parties without the express consent of FEMA or the NFIP policyholder(s) to whom the PII pertains including, as applicable, requests by third parties under state open access and freedom of information laws.

vi.   The [ENTITY SHORT NAME] shall ensure no computer matching will occur for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs unless a separate CMA is in place.

vii.   The [ENTITY SHORT NAME] will, in a timely manner, take appropriate action with regard to any request made by FEMA for access, additions, changes, deletions, or corrections of PII. In addition, the [ENTITY

SHORT NAME] will, in a timely manner, notify FEMA of any data errors that it discovers.

viii. The [ENTITY SHORT NAME] will destroy information provided by FEMA when no longer needed by [ENTITY SHORT NAME] to meet unmet needs, acquiring property, preventing duplication of benefits, or other business need as identified within this agreement.

ix. Pursuant to Routine Use N, provide FEMA with names, addresses of policyholders within their jurisdictions, and a brief general description of their plan for acquiring and relocating their flood prone properties for the purpose of ensuring that communities engage in floodplain management, improved real property acquisitions, and relocation projects that are consistent with the NFIP.

6. **CONSENT TO THIRD PARTY ACCESS TO NFIP POLICYHOLDER PII**:

Subject to the restrictions and limitations set forth in this ISAA, FEMA authorizes [ENTITY SHORT NAME] to share NFIP policyholder PII with [CONTRACTOR LONG NAME (SHORT NAME)] pursuant to the Contract Number xxxxx between the [ENTITY SHORT NAME] and [CONTRACTOR SHORT NAME] dated [DATE]. The data will be used to [CITE SPECIFIC USE]. [CONTRACTOR SHORT NAME] may not share the information with any of its subcontractors or third-party partners. [CONTRACTOR SHORT NAME] may only use NFIP policyholder PII for the purposes outlined in Contract Number xxxxx (copy of the contract must be attached).

[ENTITY SHORT NAME] shall limit its sharing of PII to contractors on a need to know basis to those employees working for the above-named state agencies who have a need to know in the performance of their official duties.

NOTE: Before you skip over this section, please consider the fact that anyone who is not a direct employee of the municipality would be considered a third-party user. If you contract out for floodplain management, engineering, CRS administration, etc. these are considered "third party" users. If you have an MOU with another community to provide floodplain management or engineering services, this would be considered "third party" use. If you are sharing address data with a County agency coordinating mitigation grants or a planning firm writing a Hazard Mitigation Plan, these would be considered "third party" users.

If no third party is noted, then paragraph 6 should read:
CONSENT TO THIRD PARTY ACCESS TO NFIP POLICYHOLDER PII:

At this time, [ENTITY SHORT NAME] has not indicated an intent to share NFIP policyholder PII with third party contractors.

7. **POINTS OF CONTACT.**

   a. The FEMA points of contact are as follows:

      Monique Crewes
      Acting Chief, Insurance Analytics and Policy, FIMA
      202-655-8573
      Monique.Crewes@fema.dhs.gov

      Scott McAfee
      GIS Analyst, FIMA
      202-236-3255
      Scott.Mcafee@fema.dhs.gov

      Marianne Luhrs
      FEMA Regional Pivot Administrator
      DHS/FEMA Region II
      347-515-4874
      Marianne.Luhrs@fema.dhs.gov

   b. The [ENTITY SHORT NAME] points of contact are as follows: (No more than five POCs)

      NAME
      TITLE
      TELEPHONE NUMBER
      EMAIL ADDRESS

8. **SEVERABILITY.** Nothing in this ISAA is intended to conflict with current law, regulation, or FEMA directives. If a term of this ISAA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this ISAA shall remain in full force and effect.

9. **NO PRIVATE RIGHT.** This ISAA is an internal agreement between FEMA and the [ENTITY SHORT NAME]. It does not create nor confer any right or benefit that is substantive or procedural, enforceable by any third party against the Parties, the United States, or other officers, employees, agents, or associated personnel thereof. Nothing in this ISAA is intended to restrict the authority of either party to act as provided by law, statute, or regulation, or to restrict any party from administering or enforcing any laws within its authority or jurisdiction. Accordingly, the terms of this Agreement do not constitute or imply the grant, by the United States of America, of any other consent, accord, satisfaction, advice, or waiver of its rights, power or authority.

10. **FUNDING.** This ISAA is not an obligation or commitment of funds, nor a basis for transfer of funds. Each party shall bear its own costs in relation to this ISAA. Expenditures by each party will be subject to its budgetary processes and to availability of funds pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

11. **ISSUE RESOLUTION.** FEMA and the [ENTITY SHORT NAME] understand that during the course of this ISAA, they may have to resolve issues such as: scope, interpretation of provisions, unanticipated technical matters, and other proposed modifications. Both parties agree to appoint their respective points of contact to work in good faith towards resolution of such issues.

12. **USE OF CONTRACTOR WITH ACCESS TO NFIP POLICYHOLDER PII.** When the [ENTITY SHORT NAME] utilizes a contractor in connection with its performance of its obligations under the ISAA and the [ENTITY SHORT NAME] provides such contractor with access to NFIP policyholder PII, the [ENTITY SHORT NAME] shall provide FEMA with prompt notice of the identity of such contractor and the extent of the role that such contractor will play in connection with the purpose of this ISAA. Moreover, all such contractors given access to any NFIP policyholder PII must agree to: (a) abide by the conditions set forth herein, including, without limitation, its provisions relating to compliance with minimum standards for the protection of NFIP policyholder PII and Notice of Security and/or Privacy Incident; (b) restrict use of NFIP policyholder PII only to the performance of services to [ENTITY SHORT NAME] in connection with [ENTITY SHORT NAME] performance of its obligations under the ISAA, and (c) certify in writing, upon completion of the performance of services by a contractor, that the contractor has immediately un-installed, removed, and/or destroyed all copies of NFIP policyholder PII within 30 days of the contractor's performance of services to the [ENTITY SHORT NAME].

13. **RETURN OR DESTRUCTION OF NFIP POLICYHOLDER PII.** If at any time during the term of the ISAA any part of NFIP policyholder PII, in any form, that the [ENTITY SHORT NAME] obtains from FEMA ceases to be required by the [ENTITY SHORT NAME] for the performance of the purpose under the ISAA, or upon termination of the ISAA, whichever occurs first, [ENTITY SHORT NAME] shall, within fourteen (14) days thereafter, promptly notify FEMA and securely return the NFIP policyholder PII to FEMA, or, at FEMA's written request destroy, un-install and/or remove all copies of such NFIP policyholder PII in the [ENTITY SHORT NAME]'s possession or control, and certify to FEMA that such tasks have been completed.

14. **ENTIRE AGREEMENT**. This ISAA constitutes the entire agreement between the parties with regard to information sharing.

15. **MODIFICATION**. This ISAA may be modified upon the mutual written consent of the parties.

16. **COUNTERPARTS.** This ISAA, when executed in any number of counterparts and by different parties on separate counterparts, each of which counterparts when so executed and delivered shall be deemed to be an original, and all of which counterparts taken together shall constitute but one and the same Agreement.

17. **EFFECTIVE DATE**, **DURATION AND TERMINATION.** This ISAA will become effective upon the signature of both parties and will remain in effect for three years. However, FEMA will only provide the information identified in Appendix A for the disaster period of assistance. Either party may terminate this agreement upon written notice to the other party.

18. **NOTICE OF PRIVACY INCIDENT**. If the [ENTITY SHORT NAME], or its contractors, suspect, discover or are notified of a suspected or confirmed privacy incident relating to NFIP policyholder PII, the [ENTITY SHORT NAME] shall immediately, but in no event later than twenty-four (24) hours from suspicion, discovery or notification of the suspected or confirmed privacy incident, notify the FEMA Privacy Officer at (202) 212-5100 or FEMA-Privacy@fema.dhs.gov.

19. **PRIVACY INCIDENT HANDLING.** In the event of a privacy incident emanating from this ISAA, FEMA will investigate the incident pursuant to DHS standard procedures and will consult [ENTITY SHORT NAME] to diagnose, mitigate and manage the privacy incident. The [ENTITY SHORT NAME] will be responsible for carrying out all necessary measures to remedy the effects of the privacy incident.

20. **REPORTING**. This ISAA covers several routine uses outlined in Paragraph 3 (d) and (e). Each time a record is requested under this ISAA, [ENTITY SHORT NAME] will indicate the specific purpose and use of the record and the specific routine use under which the record is being requested. FEMA will keep a record of the date, nature, and purpose of each disclosure of a record under this ISAA. The Parties will coordinate to prepare a report/audit summarizing compliance with the privacy, redress, and security requirements set forth in this Agreement.

21. **INDEMNIFICATION.** The [ENTITY SHORT NAME] shall bear all costs, losses and damages to the extent resulting from [ENTITY SHORT NAME] breach of the ISAA. [ENTITY SHORT NAME] agrees to release, defend, indemnify, and hold harmless FEMA for claims, losses, penalties and damages and reasonable attorneys' fees and costs to the extent arising out of [ENTITY SHORT NAME]'s, or its contractor's, negligence, unauthorized use or disclosure of NFIP policyholder PII and/or [ENTITY SHORT NAME]'s, or its contractor's, breach of its obligations under the ISAA. [ENTITY SHORT NAME] shall inform all of its principals, officers, employees, agents and contractors assigned to handling NFIP policyholder PII under the ISAA of the obligations contained in the ISAA.

22. PENALTIES. The [ENTITY SHORT NAME] understands that if it or one of its employee/agents willfully discloses any such PII to a third party not authorized to receive it, FEMA will revoke the [ENTITY SHORT NAME]'s access to NFIP policyholder PII.

APPROVED BY:

FEDERAL EMERGENCY MANAGEMENT AGENCY

_____   _____

Cynthia Spishak   Date
Federal Insurance Directorate Deputy Assistant Administrator
DHS/FEMA/Resilience/FIMA

[ENTITY LONG NAME]

_____   _____

NAME OF PERSON WITH AUTHORITY TO SIGN   Date
TITLE
ENTITY LONG NAME

Appendix A – NFIP Data Description

The following lists the NFIP policyholder PII data elements that may be shared by FEMA with the [ENTITY SHORT NAME]. The [ENTITY SHORT NAME] will only receive the PII data, or data when combined with other data could lead to PII, necessary to meet the routine use:

- Property Address
- Date of Loss
- Building Characteristics
- Coverages (building, contents)
- Premium and fees
- Claims amount paid (building, contents, ICC)
- Non-PII data elements as necessary, requested, and available

NFIP System of Records Notices (SORNs) Routine Uses

A	To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:
	    1. DHS or any component thereof;
	    2. Any employee or former employee of DHS in his/her official capacity;
	    3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or
	    4. The U.S. or any agency thereof.

B	To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.
C	To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.
D	To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E	To appropriate agencies, entities, and persons when:
	    1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;
	    2. DHS has determined that as a result of the suspected or confirmed

	compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and 3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.
F	To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or assignment for DHS, when necessary to accomplish an agency function related to this system of records. Any individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.
G	To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.
H	To Write Your Own insurance companies as authorized under 44 CFR 62.23 to administer flood insurance in partnership with FEMA.
I	To federal, state, local, and tribal government agencies, insurance companies, and established voluntary organizations in order to determine eligibility for benefits, verify non-duplication of benefits following a flooding event or another disaster, and provide needs unmet by NFIP claims payouts within their jurisdictions and service areas.
J	To state government agencies in order to provide GFIP certificates for carrying out the purposes of the NFIP within its jurisdiction.
K	To property loss reporting bureaus, state insurance departments, and insurance companies to investigate fraud or potential fraud in connection with claims, subject to the approval of the DHS Office of the Inspector General.
L	To state, local, and tribal government agencies to ascertain the degree of financial burdens they expect to assume in the event of a flooding disaster within its jurisdiction.
M	To state, local, and tribal government agencies to further NFIP outreach and education activities within their jurisdiction.
N	To state, local, and tribal government agencies that provide names, addresses of policyholders within their jurisdictions, and a brief general description of their plan for acquiring and relocating their flood prone properties for the purpose of ensuring that communities engage in floodplain management, improved real property acquisitions, and relocation projects that are consistent with the NFIP. This is contingent upon the Federal Insurance Mitigation Administration determining that the use furthers the flood plain management and hazard mitigation goals of the agency.

O	To the Army Corps of Engineers and federal, state, local, and tribal government agencies to review NFIP policy and claims information for properties within its jurisdiction in order to assist in hazard mitigation and floodplain management activities, and in monitoring compliance with the floodplain management measures adopted by the community.
P	To lending institutions and mortgage servicing companies for purposes of assisting with lender compliance.
Q	To current owners of properties for the purpose of providing the dates and dollar amounts of past loss payments made to the said property.
R	To federal, state, local, and tribal government agencies to conduct research, analysis, and feasibility studies of policies and claims within its jurisdiction.
S	To financial institutions for purposes of providing referral or cooperative reimbursement payments to insurance agents to share marketing and advertising costs between NFIP and entities participating in the NFIP.
T	To community officials and representatives to provide repetitive loss records of properties within that community.
U	To OMB in for purposes related to the review of private relief legislation in accordance with OMB Circular No. A-19.
V	To private reinsurers, private capital firms, and financial institutions for the purposes of preparing NFIP assumption of risk proposals.
W	To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

https://www.gpo.gov/fdsys/pkg/FR-2014-05-19/html/2014-11386.htm

Instructions

All yellow highlighted sections in the template need to be completed. If a section is stricken I recommend you delete it. Please see notes in boxes with red font. They should be deleted from your final Information Sharing Access Agreement (ISAA). Once you determine the applicable section in blue highlight, please delete the non-applicable section and remove the highlights.

For your POCs, you may list up to (but no more than) five community officials or staff. Please note you may modify the POCs or add POCs under #6 at a later date.

Under #6, you must identify contractors that you intend on sharing the Personally Identifiable Information (PII) NFIP data with. However, you must demonstrate that the

contract and the services being performed are tied to an appropriate routine use activity. Under #6, you must include:
1. Name of the firm
2. Contract number
3. Signed copies of all contracts referenced in #6 must accompany the ISAA.
4. Brief description of the work the firm is doing (you can look at the last few pages of the template for the applicable routine uses). If you compare the **sample approved language below** with the template language you will get a sense of the info you need to include.

Sample Approved Language on Third Party Users
6. CONSENT TO THIRD PARTY ACCESS TO NFIP POLICYHOLDER AND CLAIMS PII:
FEMA authorizes PRDOH to share NFIP policyholder PII with Company #1 (agreement DOH-RFP-17-18-01) and Company #2 (2019-000003) for them to perform work related to Hurricanes Irma and Maria. Company #1 will use the PII and associated data to support PRDOH in developing and administering Community Development Block Grants that PRDOH received from the U.S. Department of Housing and Urban Development for disaster recovery activities and reviewing its Action Plan to assess unmet needs. Company #2 will be developing the software system that will handle the NFIP policyholder PII and associated data and Company #2 will enter the NFIP policyholder PII and associated data into PRDOH's system.   PRDOH must ensure that Company #1 and Company #2 use and maintain NFIP PII in accordance with this ISAA. Company #1 and Company #2 may not share the NFIP PII with any of its subcontractors or third-party partners nor with any other government or non-government entities or individuals. Company #1 and Company #2 may only use NFIP policyholder PII for the purposes outlined in this ISAA and their contract/agreement.

To start the process, the jurisdiction must complete the ISAA template and send it to HQ's NFIP Insurance Analytics & Policy Branch (IAPB) at FEMA-NFIP-IAP@fema.dhs.gov for review. The email subject line should read *ISAA_ [External Entity Name]_R2_[date].* You may CC chanelle.lacross@fema.dhs.gov and marianne.luhrs@fema.dhs.gov . Only after IAPB has approved the ISAA language, the jurisdiction's Chief Elected Official or appropriate designee may sign the ISAA. The signed ISAA should then be forwarded to FEMA-NFIP-IAP@fema.dhs.gov, CC to chanelle.lacross@fema.dhs.gov and marianne.luhrs@fema.dhs.gov. The ISAA will then be signed by the Assistant Administrator or the Deputy Assistant Administrator for the Federal Insurance & Mitigation Administration (FIMA) and it will be uploaded to the Insurance Analytics and Policy Branch (IAPB) repository.

Once your ISAA is signed and uploaded to the IAPB repository, we will provide you with guidance on the next step – submitting your NFIP data request to FEMA.

Please note that this template has been approved by the internal legal and privacy offices at FEMA and DHS. If you initiate changes to the ISAA language, those

offices will need to review the document again and your changes may not be approved.