Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Integrated Public Alert and Warning System (IPAWS) – Memorandum of Agreements**		
Component:	Federal Emergency Management Agency (FEMA)	**Office or Program:**	Protection and National Preparedness (PNP)/ National Continuity Programs (NCP)/IPAWS
Xacta FISMA Name (if applicable):	**N/A**	**Xacta FISMA Number (if applicable):**	**N/A**
Type of Project or Program:	**Form or other Information Collection**	**Project or program status:**	**Operational**
Date first developed:	**January 17, 2012**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	**N/A**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	**Not started**	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	**Antwane Johnson**		
Office:	**PNP/NCP/IPAWS**	**Title:**	Division Director
Phone:	**202-646-4383**	**Email:**	Antwane.johnson@fema.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**N/A**		
Phone:	**N/A**	**Email:**	N/A

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA
During an emergency, alert and warning officials need to provide the public with life-saving information quickly. FEMA's Protection and National Preparedness (PNP), National Continuity Programs (NCP) owns and operates Integrated Public Alert and Warning System (IPAWS), a modernization and integration of the nation's alert and warning infrastructure that saves time when time matters most in protecting life and property. Federal, state, local, tribal and territorial alerting authorities can now use IPAWS and integrate local systems that use Common Alerting Protocol (CAP) standards with the IPAWS infrastructure. IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and other public alerting systems from a single interface. A federal, state, territorial, tribal, or local alerting authority that applies for authorization to use IPAWS is designated as a Collaborative Operating Group (COG) by the IPAWS Program Management Office (PMO). To become a COG, a Memorandum of Agreement (MOA) governing system security must be executed between the sponsoring organization and FEMA. Once, FEMA receives the hard copy IPAWS application, it is scanned into an electronic format on FEMA's common drive, which is a FEMA controlled network server, and is restricted to select FEMA IPAWS employees with an official need to know. The paper forms are then disposed of in the designated secured shred bins. The applicable and necessary information is then transferred into the IPAWS user database, which is also hosted on a FEMA controlled server. Access to the database is controlled by requiring user credentials, i.e. username and password. In addition, the user information in the IPAWS database is retrieved by the COG name. The COG name consists of the state abbreviation and name of the agency (ex. NY New York City Office of Emergency Management). Access to IPAWS is free; however, to send a message using IPAWS, an organization must procure its own IPAWS compatible software. A COG cannot sign into IPAWS, as there are no user accounts for Federal, state, territory, tribal, local government agencies. However, a COG sends a file that is digitally signed using a digital certificate that FEMA issues to the COG. The digital certificate is installed in the COG's alerting software, which has a three year expiration. A user sends an alert to IPAWS via his user profile of the "Alert Tool" they have purchased for the alerting process (profiles are unique to the user and the product they have procured).

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media

	☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these
3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☐ DHS employees/contractors (list components): ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies
4. What specific information about individuals is collected, generated or retained?	
• Name, title, and contact information of individual who signs the MOA (on behalf of sponsoring organization). Contact information includes work email address, phone number, and physical address. • Name, title, and contact information of Authorized Alerting Authority's Primary Point of Contact (POC), Alternate POC, and Technical POC. Contact information includes work email address, phone number, and physical address. • Name, title, and contact information of System Vendor/Developer for each Third-Party Interoperable Software System. Contact information includes work email address and phone number. .	
4(a) Does the project, program, or system retrieve information by personal identifier?	☒ No. Please continue to next question. ☐ Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	N/A
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	N/A
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
N/A	
5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. ☐ Yes. If yes, please list: N/A
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. Please describe applicable information sharing governance in place: N/A
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures	☒ No. What steps will be taken to develop and maintain the accounting:

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

of PII to individuals who have requested access to their PII?	☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**LaKia Samuel**
Date submitted to Component Privacy Office:	**March 5, 2015**
Date submitted to DHS Privacy Office:	July 28, 2015

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed.

IPAWS provides public safety officials with an effective platform to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and other public alerting systems from a single interface.

The Web-Portals PIA provides coverage for IPAWS for the purposes of facilitating collaborative activities within the Department that requires contact with the public as well as partners in other federal, state, local, and international governmental organizations or partners. This encompasses a wide variety of activities, to include emergency response. The GITAARS SORN covers the categories of individuals and the retrieveability of data categories for the purpose associated with the uses of the IPAWS infrastructure/collection.

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Eric M. Leckey**
PCTS Workflow Number:	**1099455**
Date approved by DHS Privacy Office:	August 7, 2015
PTA Expiration Date	August 7, 2018

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	Form/Information Collection If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	**System covered by existing PIA** If covered by existing PIA, please list: **DHS/ALL/PIA-015 - DHS Web Portals**
SORN:	System covered by existing SORN If covered by existing SORN, please list: **DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) September 29, 2009, 74 FR 49882**

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

The purpose of this PTA is to review the system, annotate the review, and determine privacy compliance coverage. IPAWS provides public safety officials with an effective platform to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA),

the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and other public alerting systems from a single interface. Privacy compliance coverage for IPAWS is provided by:

- Web-Portals PIA which provides coverage for the purposes of facilitating collaborative activities within the Department that requires contact with the public as well as partners in other federal, state, local, and international governmental organizations or partners, which encompass a wide variety of activities, to include emergency response.
- GITAARS SORN which covers the categories of individuals and the retrieveability of data categories for the purpose associated with the uses of the IPAWS infrastructure/collection.