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 – Open Platform for Emergency Networks (IPAWS-OPEN)**		
Component:	Federal Emergency Management Agency (FEMA)	**Office or Program:**	National Continuity Programs (NCP)
Xacta FISMA Name (if applicable):	**IPAWS-OPEN**	**Xacta FISMA Number (if applicable):**	**FEM-05806-MAJ-05806**
Type of Project or Program:	**IT System**	**Project or program status:**	**Operational**
Date first developed:	**August 25, 2010**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	**May 26, 2011**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	**Complete**	**ATO expiration date (if applicable):**	**August 10, 2014**

PROJECT OR PROGRAM MANAGER

Name:	**Mark Lucero**		
Office:	**IPAWS**	**Title:**	System Owner
Phone:	**202-646-1386**	**Email:**	Mark.Lucero@dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**Eric Caldwell**		
Phone:	**202-646-3109**	**Email:**	Eric.Caldwell@associates.fema.dhs.gov

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Choose an item.

Exec. Order No. 13407 requires the United States to operate an effective, reliable, integrated, flexible and comprehensive alert and warning system.. FEMA implements this policy per Exec. Order No. 13407 and has established a program office to implement the Integrated Public Alerts and Warning System (IPAWS). FEMA and its federal partners are working together to transform the national alert and warning system to enable rapid dissemination of alert information over as many communication channels as possible.

As a result, FEMA has developed the IPAWS Open Platform for Emergency Networks (IPAWS-OPEN) to enhance efficient coordination and collaboration among public safety organizations using different incident management systems. IPAWS-OPEN enables the interoperable sharing of emergency alerts and incident-related data between systems that comply with non-proprietary information standards. IPAWS-OPEN will serve the IPAWS as the IPAWS Alerts Aggregator. It will collect and route IPAWS emergency alerts to and from emergency systems that serve the public. This system will integrate with the various alert dissemination methods and its web based services design will allow for the addition of future alert and warning systems.

IPAWS-OPEN provides integrated services and capabilities to local, state and federal authorities that enable them to alert and warn their respective communities via multiple communications methods. IPAWS-OPEN is an interoperability backbone available to the emergency responder community. The system is an open point of exchange offering non-proprietary "level playing field" web services as a method of removing barriers to entry for systems wishing to implement messaging standards. As a Federal infrastructure, IPAWS-OPEN ensures the delivery of real-time data and situational awareness to public emergency responders in the field, at operation centers, and across all levels of response management.

IPAWS-OPEN exists as a web-based message brokering service that provides Emergency Managers a space to create messages using various messaging protocols and standards. IPAWS-OPEN is the backbone system that structures the alert and distributes the message from one interoperating and/or interconnected system (message sender) to another interoperating and/or interconnected system (message recipient). IPAWS-OPEN is not directly accessible by end users as end users must use these interoperable or interconnected systems to originate and receive messages.
IPAWS-OPEN will support the following three basic Web services through Application Programming Interfaces:
• Common Alerting Protocol (CAP): Enables the exchange of emergency alerts utilizing CAP-compliant enabled systems.
• Non-weather Emergency Messaging (NWEM): A specialized form of CAP alert distributed by the National Weather Service and relayed to the Emergency Alert System.
• Distribution Element (EDXL-DE): Routes content, including Resource Messages (EDXL-RM)*, Hospital Availability Exchange (EDXL-HAVE)* messages, National Information Exchange Model (NIEM)-

compliant content, and other commonly defined file types. FEMA is submitting this PTA as the system is undergoing recertification (existing PTA approved in October 2011). No changes have been made to the system that impact PII.

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?	
This system does not contain any such information.	
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:

[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(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
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.	
Click here to enter text.	

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: Click here to enter text.
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:

[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.

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 of PII to individuals who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: N/A ☐ 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

[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.

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

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Kathryn Fong**
Date submitted to Component Privacy Office:	**April 23, 2014**
Date submitted to DHS Privacy Office:	July 1, 2014
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
Consistent with the existing PTA approved in Oct. 2011, this system does not collect or use PII. Therefore, FEMA Privacy recommends that it be adjudicated as non-privacy sensitive.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Jameson A. Morgan**
PCTS Workflow Number:	**1025852**
Date approved by DHS Privacy Office:	July 14, 2014
PTA Expiration Date	July 14, 2017

DESIGNATION

Privacy Sensitive System:	No If "no" PTA adjudication is complete.
Category of System:	Other If "other" is selected, please describe: web-based message brokering service

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:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.

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

The DHS Privacy Office agrees with the FEMA Privacy Office that IPAWS – OPEN is a non-privacy sensitive system. No further privacy documentation or coverage is required by the Privacy Act of 1974 or the E-Government Act of 2002.

This PTA was submitted because the system is undergoing recertification. There have not been any significant changes to the system since the last PTA adjudication in 2011, and there have not been any changes that implicate PII.

IPAWS-OPEN is not directly accessible by end users and is the backbone system that structures alerts and distributes messages from one interoperating or interconnected system to another interoperating or interconnected system. IPAWS-OPEN is a web-based message brokering service that allows FEMA to create messages using various messaging protocols and standards.

This PTA is sufficient because IPAWS-OPEN does not collect, use, maintain, or disseminate any PII.