Privacy Impact Assessment
for the

Integrated Public Alert Warning System - Open Platform for Emergency Networks (IPAWS-OPEN)

DHS/FEMA/PIA-046

July 17, 2017

Contact Point
Mark Lucero
IPAWS-OPEN, Chief
Federal Emergency Management Agency
(202) 646-1386

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) operates and directs the Integrated Public Alert and Warning System – Open Platform for Emergency Networks (IPAWS-OPEN). This system provides integrated services and capabilities to federal, state, local, tribal, and territorial agencies (Alerting Authorities) that enable them to alert and warn their respective communities via multiple communication methods. IPAWS-OPEN ensures the delivery of real-time data and situational awareness to the public, public emergency responders in the field, at operation centers, and across all levels of response management. FEMA is conducting this Privacy Impact Assessment (PIA) because IPAWS-OPEN collects, stores, transmits, and disseminates several types of alerts and warnings, including America's Missing: Broadcast Emergency Response (AMBER) alerts that contain personally identifiable information (PII).

Overview

Executive Order No. 13407 requires the United States to operate an effective, reliable, integrated, flexible, and comprehensive alert and warning system. To meet the requirements of this Executive Order, FEMA 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.

FEMA developed the IPAWS-OPEN system to enhance efficient coordination and collaboration among Alerting Authorities across various jurisdictions that operate different incident management systems. IPAWS-OPEN enables the interoperable sharing of emergency alerts incident-related data between systems that comply with Common Alerting Protocol (CAP).[1] IPAWS-OPEN serves as the IPAWS Alerts Aggregator/Gateway. It collects and routes IPAWS emergency alerts to and from emergency systems that serve the public. Alerts are sent through the IPAWS Alert Aggregator/Gateway, then disseminated to the different public alerting systems using Hypertext Transfer Protocol Secure (HTTPS).[2] The IPAWS Alert Aggregator/Gateway authenticates the Alerting Authority, validates the CAP message, verifies permissions, and ensures that the message has not been altered during transmission using digital signatures.[3] IPAWS-OPEN

[1] The Common Alerting Protocol (CAP) is a digital format for exchanging emergency alerts that allows a consistent alert message to be disseminated simultaneously over many different communications systems.
[2] HTTPS is a protocol for secure communication over a computer network that is widely used on the internet.
[3] IPAWS-OPEN ensures message integrity and non-repudiation for posting by digitally signing the Simple Object Access Protocol (SOAP) message using XML digital signature specification.

interfaces with the various alert dissemination methods. Its web-based services design allows for the addition of future alert and warning systems.

The Alerting Authorities' external interoperating systems use standards-based web services to establish interfaces to IPAWS-OPEN. These systems can include other incident management systems as well as other alert and message distribution systems. The IPAWS-OPEN Services Oriented Architecture (SOA)[4] platform can be viewed as an enterprise messaging system, which allows integration between different architectures without the need for writing code through the use of interface adapters and data transformation services. IPAWS-OPEN enables the following services: 1) IPAWS CAP Alert Aggregator Service; and 2) Emergency Data Exchange Language – Distribution Element (EDXL-DE). The IPAWS CAP Alert Aggregator Service provides interfacing systems with the ability to post alerts and warnings to relevant public alerting systems.[5] Each channel disseminates the message to the appropriate or relevant audience.

EDXL-DE provides the capability for interfacing systems to post messages to IPAWS-OPEN and share with other interfacing systems. The EDXL-DE capability provides IPAWS Collaborative Operating Groups (COG)[6] with the ability to send and receive messages with other users or relevant parties. EDXL-DE allows messages to be characterized by content type, sender organization type, desired receiving organization type, or geographic area of interest to determine who should receive the message. Each of these services provides the Alerting Authority with the ability to submit messages to IPAWS-OPEN to be shared with other COGs and dissemination channels, as well as the ability to recall messages for any reason.

Any Alerting Authority applying for authorization to use IPAWS-OPEN to send alerts to the public must first go through a vetting process. First, an Alerting Authority must execute a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) with FEMA.[7] All MOAs/MOUs contain Interconnection Security Agreements (ISA) as well as Rules of Behavior (ROB). Each MOA/MOU is specifically tailored to the Alerting Authority and its interoperable alert origination system. Second, FEMA must verify that an Alerting Authority has procured its own IPAWS-OPEN-compatible alert origination software. Third, the Alerting Authority must apply for alerting permission by completing an application that indicates the types of dissemination

[4] SOA describes an IT infrastructure that allows different applications to exchange data with one another as they participate in business processes.
[5] Emergency Alert System (EAS), Wireless Emergency Alert System (WEAS), Commercial Mobile Alerting System (CMAS), National Weather Service (NWS)-HazCollect system, National Oceanic and Atmospheric Administration (NOAA) Weather Radio, Internet Services, and State/Local Unique Alerting Systems.
[6] A Collaborative Operations Group (COG) is a virtual organization of users who agree to dynamically create and share information amongst themselves in real time. More specifically in terms of emergency management functions, a COG typically is a voluntary incident or consequence management organization consisting of emergency response officials who need to coordinate actions, communicate, and exchange information in a collaborative environment. COGs are assigned identification numbers to effectuate the sending and receiving of messages.
[7] FEMA Forms 007-0-025 and 007-0-026, included in OMB Control Number 1660-0140, are IPAWS MOA forms. These forms fall under the scope of the IPAWS program.

systems, the extent of the geographic warning area in their jurisdiction, and the event codes they intend to use. Finally, all Alerting Authorities are required to complete IPAWS-OPEN web-based training. FEMA's Emergency Management Institute offers the independent study course entitled, "IS-247.A, IPAWS."[8]

IPAWS-OPEN does not allow for the public to directly access the system. All message originators and recipients (i.e., users) of the message aggregration and dissemination capabilities within IPAWS-OPEN must use a system or application that is connected to or interoperating with IPAWS-OPEN. These interconnected and interoperable systems include: 1) Emergency Alert System (EAS) Broadcaster systems; 2) Commercial Mobile Service Providers' (CMSP) systems; 3) interoperating applications owned and operated by emergency management organizations; and 4) other interconnected systems such as HazCollect, which is owned and operated by National Oceanic and Atmospheric Administration's (NOAA) National Weather Service.

The FEMA IPAWS-OPEN program personnel maintain the IPAWS-OPEN system. The IPAWS-OPEN program personnel audit alerts and messages on an ad hoc basis to ensure that data is used for authorized purposes consistent with the original purpose of the collection. All IPAWS-OPEN program personnel have role-based access. Before program personnel can access the IPAWS-OPEN system, the system owner manually creates a username and temporary password and provides it to the new employee. The system owner assigns the employee's level of access and permissions. Once a new employee logs into his or her account for the first time, he or she is immediately prompted to reset his or her temporary password. Once FEMA establishes the IPAWS-OPEN account, every time the employee logs into IPAWS-OPEN system it verifies the employee's credentials and logs his or her activity.

The IPAWS-OPEN system sends out multiple types of public alert and warning messages. The messages and alerts include: avalanche, blizzard, earthquake, fire, flash flood, hurricane, tornado, and dust storm warnings; law enforcement warnings; local area emergencies alerts; nuclear power plant warnings; radiological hazard alerts; shelter-in-place warnings; civil emergency messages; and AMBER alerts.

AMBER alerts[9] are the only alerts containing PII that the IPAWS-OPEN system collects, stores, and transmits. The PII in AMBER alerts is needed to assist law enforcement in the safe

[8] https://training.fema.gov/is/courseoverview.aspx?code=is-247.a.

[9] The U.S. Justice Department's Guidance on Criteria for Issuing AMBER Alerts is as follows:

- There is reasonable belief by law enforcement that an abduction has occurred;
- The law enforcement agency believes that the child is in imminent danger of serious bodily injury or death;
- There is enough descriptive information about the victim and the abduction for law enforcement to issue an AMBER Alert to assist in the recovery of the child;
- The abduction is of a child aged 17 years or younger; and
- The child's name and other critical data elements, including the Child Abduction flag, have been entered

return of abducted children. AMBER alerts data include name of the abducted child, name of potential suspect(s), home addresses, email addresses, telephone numbers, license plates numbers, photographic images, and distinguishing characteristics. AMBER alerts are stored in IPAWS-OPEN for forensic purposes and sorted by a unique IPAWS message identifier number. The IPAWS message identifier number does not relate to individuals but rather to the message itself. All messages sent to the IPAWS-OPEN are randomly assigned an IPAWS message identifier number. AMBER alerts are maintained along with other IPAWS-OPEN messages and alerts in a database and will be purged in accordance with forthcoming National Archives and Records Administration (NARA) retention schedule. As there is no NARA retention schedule, FEMA currently retains AMBER alerts permanently. Out of 992,060 IPAWS-OPEN messages disseminated in 2016, less than 1 percent of all IPAWS-OPEN messages are AMBER alerts.[10]

IPAWS-OPEN System Typical Transaction

A typical transaction requires Alerting Authorities to create a CAP-compliant alert in their external interoperating system. This alert can range from an AMBER alert to a tornado warning. Once the Alerting Authority generates the alert, it sends it to the IPAWS-OPEN system using HTTPS. On receipt of the alert, IPAWS-OPEN authenticates the sender, validates the alert, verifies permissions, and ensures that the alert has not been altered during transmission by using digital signatures. IPAWS-OPEN then disseminates the alert to relevant public alerting systems.[11] The relevant public alerting systems then disseminate the alert to radio stations, television stations, cellular phone carriers, and highway message boards to broadcast the alert to the public.

IPAWS-OPEN keeps a record of each alert in its database and those alerts are sorted using a unique message identifier that is issued by IPAWS-OPEN. If Alerting Authorities request this data, IPAWS-OPEN program personnel respond by searching the IPAWS-OPEN system via the unique message identifier to locate the records. All information processed by the IPAWS-OPEN system is determined by the Alerting Authority to be suitable for public dissemination and public release. FEMA does not have authority to change the messages created by the Alerting Authorities, nor does FEMA own the messages or alerts. Additionally, one Alerting Authority cannot access another Authority's alerts. FEMA's role is limited to maintaining the IPAWS-OPEN system and providing this alerting service to the end users.

---

into the National Crime Information Center (NCIC) system.

[10] 158 AMBER alerts were disseminated in IPAWS-OPEN in 2016.

[11] These systems are: Emergency Alert System (EAS), Wireless Emergency Alert System (WEAS), National Oceanic and Atmospheric Administration (NOAA) Weather Radio, Internet Services, State/Local Unique Alerting Systems.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Homeland Security Act of 2002, as amended; [12] Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended; [13] Executive Order No. 13407; [14] Communications Act of 1934, as amended;[15] and IPAWS Modernization Act of 2015[16] authorize the collection of information in IPAWS-OPEN.

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

Through the IPAWS-OPEN authentication process, the system retrieves program personnel system permissions by username and password. The collection and storage of this information is covered by DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORN.[17]

The messages and alerts received, stored, and shared by IPAWS-OPEN are not subject to the requirements of the Privacy Act of 1974 because IPAWS-OPEN messages and alerts are not retrieved by personal identifier. IPAWS-OPEN messages and alerts are retrieved by a unique message identifier not linked to an individual.

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

The Authority to Operate (ATO) was issued on September 23, 2016, and is currently undergoing recertification.

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

FEMA's Records Management Branch is collaborating with the IPAWS-OPEN system owner and NARA to establish an approved retention and disposal schedule for the messages and alerts contained in IPAWS-OPEN that is consistent with the mission-driven needs of the agency. This data will be retained until the retention schedule is approved. This PIA will be updated and

[12] 6 U.S.C. §§ 311-321m.
[13] 42 U.S.C. §§ 5121-5207.
[14] Exec. Order No. 13407, 71 FR 36975 (2006).
[15] 47 U.S.C. § 606.
[16] Pub. L. No. 114-143, 130 Stat. 327 (2016).
[17] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (Nov. 27, 2012).

all data will be retained and disposed of in accordance with the NARA-approved schedule, including retroactively, once NARA has approved the retention and disposal schedule.

The records retention schedule for access credentials of IPAWS-OPEN program personnel has been approved by the FEMA Records Officer and NARA as Authorities GRS 3.2, Item 031. Inactive username and password records will be destroyed or deleted 6 years after the user account is terminated or password is altered, but longer retention is authorized if required for business use.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

IPAWS-OPEN is not subject to PRA requirements because the system does not solicit information from the public. Alerting Authorities provide the information contained in the alerts that are disseminated to the public on a voluntary basis.[18]

Section 2.0 Characterization of the Information

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

IPAWS-OPEN messages/alerts related to natural or manmade disasters contain information related to the incident, and do not contain PII. They include:

- Emergency event type (e.g., avalanche, blizzard, earthquake, AMBER Alerts);
- Emergency event location;
- Emergency severity; and
- Evacuation details.

PII may be included in the AMBER alerts only, which include:

- Name of abducted child;
- Name of potential suspects;
- Gender;

[18] The IPAWS program, not the IPAWS-OPEN system, does have information collections that fall under the PRA. FEMA Forms 007-0-025 and 007-0-026, included in OMB Control Number 1660-0140, are IPAWS MOA forms.

- Street address information;
- Contact information, including telephone numbers (mobile, business, and home) and email address;
- License plate number;
- Business telephone number of responding police department; and
- Personal characteristics of the abducted child or potential suspects, including photographic images (specifically of face or other distinguishing characteristics).

PII collected from IPAWS-OPEN program personnel to create an IPAWS-OPEN account:

- Username; and
- Password.

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

The information contained in the alerts and messages is collected indirectly from Alerting Authorities. The Alerting Authorities input the information in their respective external operating system, create the desired alert, and send it to the IPAWS-OPEN system via HTTPS. DHS collects the usernames and passwords directly from IPAWS-OPEN program personnel.

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

IPAWS-OPEN does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

FEMA does not verify the accuracy of the alerts. FEMA assumes the information provided by the Alerting Authorities is accurate. IPAWS-OPEN authenticates the sender, validates the AMBER alert using a digital signature certificate, verifies permissions, and ensures that the AMBER alert has not been altered during transmission by using digital signatures.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the data within IPAWS-OPEN may be inaccurate due to its reliance on alert information submitted by Alerting Authorities.

Mitigation: FEMA does not mitigate this risk. IPAWS-OPEN assumes the accuracy of the

alert information it receives from Alerting Authorities. If an Alerting Authority sends an alert with inaccurate information, it has the ability to cancel the alert, update it, and re-send the alert. The Alerting Authority is responsible for catching any errors and making any updates.

Privacy Risk: There is a privacy risk that PII is unnecessarily included in the alert and disseminated through the alert system.

Mitigation: FEMA does not mitigate this risk. The burden of mitigation rests with the Alerting Authorities, which are required to follow specific guidelines regarding sending alerts to the IPAWS-OPEN system as specified in executed ISAs with FEMA. With the exception of AMBER alerts, the executed ISAs require Alerting Authorities to send alerts devoid of PII, financial, classified, or law enforcement sensitive information. Alerting Authorities will only send alerts containing the information necessary to warn or alert the public of national disasters, weather events, hazardous material events, and abducted children.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends FEMA conduct regular spot audits to ensure that the guidelines are being met and that PII is not inadvertently being included in the alerts.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

IPAWS-OPEN disseminates alerts and messages it receives from Alerting Authorities in order to warn or alert the public of national disasters, weather events, hazardous material events, and abducted children. Alerting Authorities create a CAP-compliant alert in their external interoperating system. This alert can range from an AMBER alert to a tornado warning. Once the Alerting Authority generates the alert, it sends it to the IPAWS-OPEN system using HTTPS. On receipt of the alert, IPAWS-OPEN authenticates the sender, validates the alert, verifies permissions, and ensures that the alert has not been altered during transmission by using digital signatures. IPAWS-OPEN then disseminates the alert to relevant public alerting systems. The relevant public alerting systems then disseminate the alert to radio stations, television stations, cellular phone carriers, and highway message boards to broadcast the alert to the public.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

IPAWS-OPEN does not, and will not, use technology to conduct electronic searches, queries, or analysis to discover or locate predictive patterns or anomalies.

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

No other DHS component has an assigned role or responsibility within the IPAWS-OPEN system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the system could be used to embarrass or harm an individual by disseminating his or her information through IPAWS-OPEN.

Mitigation: This risk is partially mitigated by the limited access to the IPAWS-OPEN system. Only Alerting Authorities and IPAWS-OPEN program personnel have access to the IPAWS-OPEN system. Alerting Authorities are the only entities that can disseminate information though the IPAWS-OPEN system. Alerting Authorities are only granted access to the IPAWS-OPEN system after they complete a four-step vetting process. Additionally, IPAWS-OPEN program personnel maintain the IPAWS-OPEN system and audit alerts and messages on an ad hoc basis to ensure that data is used for authorized purposes consistent with the original purpose of the collection.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

FEMA is publishing this PIA to serve as notice of this information collection. The website www.amberalert.gov also provides notice that AMBER alerts will be sent to FEMA for further dissemination.[19] Because FEMA is not collecting information from individuals who are the subject of the AMBER alerts, FEMA does not provide any additional notification of the information

[19] https://www.amberalert.gov/faqs.htm.

collection. Alerting Authorities may provide additional notification in accordance with applicable laws and regulations.

In addition to the PII collected in AMBER alerts, FEMA collects usernames and passwords from IPAWS-OPEN program personnel. FEMA provides notice of this collection by displaying a privacy notice on the user account request form. All IPAWS-OPEN program personnel must complete this form before being granted access to the IPAWS-OPEN system. Additionally, FEMA leverages IPAWS-OPEN training, this PIA, and the DHS/ALL-004 GITAARS SORN to ensure all program personnel receive ample notice that their information will be collected and maintained by IPAWS-OPEN.

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

Neither the abducted children, their parents, nor the potential suspects have the opportunity to opt-out of having their PII sent through IPAWS-OPEN via an AMBER alert. All information contained in AMBER alerts is sent to IPAWS-OPEN by the Alerting Authorities. The Alerting Authorities are the data owners of the AMBER alerts. IPAWS-OPEN has no interaction with the abducted children, their parents, or potentials suspects to make an opt-out option available.

IPAWS-OPEN program personnel must provide PII in order to perform their specific job duties. If PII is not provided, system access to IPAWS-OPEN cannot be granted. Therefore, IPAWS-OPEN program personnel cannot decline to provide information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that the individuals whose PII is included in IPAWS-OPEN will not receive advanced notice that their PII is being used for IPAWS-OPEN for wide dissemination at the time it is collected.

Mitigation: The privacy risk partially mitigated. The AMBER alert website, www.amberalert.gov, provides notice to the public that AMBER alerts will be sent to FEMA for further dissemination.[20] Additionally, the publishing of this PIA will provide notice to individuals that their PII is being used for IPAWS-OPEN at the time it is collected.

[20] https://www.amberalert.gov/faqs.htm.

Section 5.0 Data Retention by the project

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

FEMA's Records Management Branch is collaborating with the IPAWS-OPEN system owner and NARA to establish an approved retention and disposal schedule for the messages and alerts contained in IPAWS-OPEN that is consistent with the mission-driven needs of the agency. Currently, IPAWS-OPEN alerts and messages are kept for 90 days in the IPAWS-OPEN system. After 90 days, the messages and alerts are stored offline in database archive tables. The messages and alerts will be kept in this manner until the retention schedule is approved. This PIA will be updated and all data will be retained and disposed of in accordance with the NARA-approved schedule, including retroactively, once NARA has approved the retention and disposal schedule.

The records retention schedule for access credentials of IPAWS-OPEN program personnel has been approved by the FEMA Records Officer and NARA as Authorities GRS 3.2, Item 031. Inactive username and password records will be destroyed or deleted 6 years after the user account is terminated or password is altered, but longer retention is authorized if required for business use.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that FEMA may keep information longer than the time period necessary.

Mitigation: This risk is not yet mitigated. DHS currently minimizes the amount of time it keeps the data in line with the mission of its IPAWS-OPEN program. IPAWS-OPEN messages and alerts are currently kept for 90 days within the IPAWS-OPEN system. After 90 days, the messages and alerts are stored offline in database archive tables. The messages and alerts will be kept in this manner until a NARA retention schedule is approved, at which point the risk will be mitigated. DHS partially mitigates this risk by using advanced records management training, additional training offered by DHS and NARA, and advanced technology resources to improve records management practices and inform DHS staff of proper record retention standards.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

As an alert aggregator, IPAWS-OPEN receives alert information and shares it with the public to warn and inform them of important emergency information. These original alerts are shared with EAS, Wireless Emergency Alert System (WEAS), NOAA Weather Radio, Internet

Services, and state/local unique alerting systems. Each Alerting Authority, before they can send messages or alerts to IPAWS-OPEN, go through a DHS/FEMA-approved process to receive an account. All MOAs/MOUs and ISAs have language to ensure the joint security of the systems and the message data they store, process, and transmit. Additionally, FEMA and the receiving party agree to adhere to and enforce the security specifications defined within an ISA.

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

The purpose of IPAWS-OPEN is to disseminate alerts to the public. IPAWS-OPEN does not maintain the alerts and messages within a system of records, therefore the sharing is not done pursuant to a SORN.

6.3 Does the project place limitations on re-dissemination?

IPAWS-OPEN does not re-disseminate alerts. If a sent alert was incorrect, the Alerting Authority has the ability to cancel, correct, and re-send the alert.

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

IPAWS-OPEN maintains a record of disclosures in a shared folder outside of the system. Each scenario includes a list of recipient report types that are sent automatically, and at what interval they were sent out. Requests for IPAWS-OPEN records are made to the DHS Headquarters or FEMA Disclosure Office.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in IPAWS-OPEN could be erroneously disclosed.

Mitigation: DHS mitigates this privacy risk because DHS only shares information in IPAWS-OPEN outside of DHS pursuant through MOUs, MOAs, and ISAs vetted and approved by the FEMA Privacy Office and Office of the Chief Counsel, or pursuant to a written request submitted to the DHS Headquarters or FEMA Disclosure Office. In addition, FEMA mitigates this risk through training, as all IPAWS-OPEN program personnel receive required system training prior to gaining access to IPAWS-OPEN. Lastly, the risk associated with information sharing is mitigated through strict access control measures, as described in Section 8.3 below.

Section 7.0 Redress

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

IPAWS does not have the ability to retrieve individual records using a personal identifier, therefore it does not maintain messages and alerts within a system of record. Any requests to access information related to AMBER alerts would need to be submitted to the Alerting Authority that originated the alert. Additionally, all individuals, U.S. citizens or otherwise, seeking access to their IPAWS-OPEN account records may access their information via a Freedom of Information Act (FOIA) request to the DHS Headquarters or FEMA Disclosure Offices.

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

All information contained in IPAWS-OPEN alerts and messages originates from Alerting Authorities. Any request to correct inaccurate or erroneous information would need to be submitted to the Alerting Authority that originated the alert. If an Alerting Authority sends an alert with inaccurate information, that Alerting Authority has the ability to cancel the alert, update it, and re-send the alert. The Alerting Authority is responsible for catching any errors and making any updates.

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

This PIA provides notice regarding information correction procedures for IPAWS-OPEN.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that Alerting Authorities who send alerts to IPAWS-OPEN will be unaware of the redress process available to them.

Mitigation: DHS mitigates this privacy risk by providing notice of redress procedures in in the web-based IPAWS-OPEN training that Alerting Authorities are required to complete. This PIA also offers notice of redress to Alerting Authorities.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

FEMA ensures that the practices stated in this PIA are followed by leveraging standard

operating procedures (SOP), training, policies, Rules of Behavior (ROB), and auditing and accountability. For messages, alerts, and warnings contained in the IPAWS-OPEN system, user roles define what data a user can access. FEMA constantly monitors audits of account modifications and security operations. Modifying a record logs a security event. Administrators review logs on a weekly basis. Lastly, IPAWS-OPEN requires all Alerting Authorities to take web-based IPAWS-OPEN training, which gives an overview of IPAWS-OPEN and shows Alerting Authorities how to create, send, and recall alerts. FEMA will not allow Alerting Authorities to send messages, alert, or warnings through IPAWS-OPEN until the training is complete.

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

All FEMA employees and contractors are required to complete initial on-boarding and annual privacy awareness and security training. There is no IPAWS-OPEN-specific privacy training.

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

Only IPAWS-OPEN program personnel can access the information that is stored within the IPAWS-OPEN databases. Executed MOAs/MOUs and ISAs are entered into with Alerting Authorities that create the alerts and the public alerting systems that broadcasts the alerts. The aforementioned agreements detail the IPAWS-OPEN ROB and ensure the Alerting Authorities follow them. IPAWS-OPEN maintains access controls and separation of duties to ensure that only FEMA employees with a need to know have access to the information. The following duties all have role-based permissions: application development; testing of application services; implementation of application services; creation of Public Key Infrastructure (PKI) certificates;[21] issuance and tracking of PKI certificates; management of COG Identification Numbers; and server and database administration.

IPAWS-OPEN program data is protected through a defense-in-depth approach. Direct physical and logical access to the database is managed through access control methods including PIV-I single sign-on methods, access control at the FEMA and DHS data centers, access control at the operating system level, and access control at the application level.

[21] Public Key Infrastructure (PKI) is a comprehensive system required to provide public-key encryption and digital signature services.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

IPAWS-OPEN leverages MOUs, MOAs, and ISAs to facilitate the information exchange necessary to accomplish its mission. All MOUs, MOAs, and ISAs between FEMA and its partners are reviewed by responsible program managers, senior-level stakeholders, DHS and component privacy officers, IT security staff, and appropriate legal counsel. Finally, DHS formally reviews and approves MOUs, MOAs, and ISAs.

Responsible Officials

William Holzerland
Senior Director for Information Management
Federal Emergency Management Agency
U.S. Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

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