

**FEMA's Oversight of
the Integrated Public
Alert & Warning System
(IPAWS)**





DHS OIG HIGHLIGHTS

FEMA's Oversight of the Integrated Public Alert & Warning System (IPAWS)

November 19, 2018

Why We Did This Inspection

Following the January 13, 2018, false missile alert in Hawaii, Congress requested we examine the Federal Emergency Management Agency's (FEMA) role in the incident. As part of this review, we sought to determine whether FEMA exercises appropriate oversight of the Integrated Public Alert and Warning System (IPAWS) used to send alerts to the public.

What We Recommend

We are making two recommendations to improve the FEMA IPAWS Program Management Office's oversight of IPAWS.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

After examining FEMA's roles and responsibilities in the public alert and warning process, we concluded that FEMA has limited responsibility for the sending and canceling of state and local alerts. Although FEMA maintains IPAWS as a messaging platform, state and local alerting authorities must obtain commercially-available emergency alert software to generate a message which passes through IPAWS for authentication and delivery. However, we found that FEMA does not require that this software perform functions critical to the alerting process, such as the ability to preview or cancel an alert. Instead, FEMA only recommends that software vendors include these capabilities as "best practices." FEMA also does not require that software vendors provide training to alerting authorities on how to use their chosen software. As a result, alerting authorities have experienced difficulties in various aspects of the alerting process.

FEMA Response

FEMA concurred with the recommendations and is implementing corrective actions to enhance the effectiveness of the IPAWS Program Management Office (PMO). The IPAWS PMO will incorporate requirements for inclusion of critical functions and provisions for training into the memorandums of agreement with state, local, tribal, and territorial alerting authorities. We consider both recommendations resolved and open.




OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

November 19, 2018

MEMORANDUM FOR: The Honorable William B. Long
Administrator
Federal Emergency Management Agency

FROM: John V. Kelly 
Senior Official Performing the Duties
of the Inspector General

SUBJECT: *FEMA's Oversight of the Integrated Public Alert & Warning System (IPAWS)*

For your action is our final report, *FEMA's Oversight of the Integrated Public Alert & Warning System (IPAWS)*. We incorporated the final comments provided by your office.

The report contains two recommendations aimed at improving the overall effectiveness of IPAWS. Your office concurred with both recommendations. Based on information provided in your response to the draft report, we consider both recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of the agreed-upon corrective actions. Please send your response or closure request to OIGInspectionsFollowup@oig.dhs.gov.

Consistent with our responsibility under the Inspector General Act, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public disseminations.

Please call me with any questions, or your staff may contact Jennifer Costello, Deputy Inspector General, at (202) 981-6000.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

In the event of a disaster, state and local authorities need a way to alert and warn the people potentially in harm's way. Executive Order 13407 established policy for the United States to have a "system to alert and warn the American people in situations of war, terrorist attack, natural disaster, or other hazards to public safety and well-being."¹ In response, the Federal Emergency Management Agency (FEMA) developed the Integrated Public Alert and Warning System (IPAWS). Originally designed so the President of the United States could alert and warn the American people within 10 minutes of a national emergency, FEMA further expanded IPAWS so other Federal, state, local, tribal, and territorial authorities could send alerts and warnings to the people within their specific jurisdictions.² The *IPAWS Modernization Act of 2015* (Modernization Act) further defined FEMA's role as the Federal agency responsible for the public alert system. Specifically, the Act directed FEMA to, among other things, establish common alerting and warning protocols, standards, terminology, and operating procedures; and conduct training, tests, and exercises for the system.³

IPAWS aggregates alert and warning messages from Federal, state, local, tribal, and territorial authorities – known as alerting authorities – and delivers them to the American public through various communication methods, such as radio and television broadcasts, cellular phone messages, and Internet applications. As of February 2018, 1,030 alerting authorities, including city and county governments, sheriff's offices, emergency management offices, and police departments, could send alerts to the public. Alerts are sent for various reasons, including law enforcement situations; evacuation or shelter-in-place circumstances; extreme weather conditions; child abductions; or natural disasters, like earthquakes or wildfires.⁴ From April 2012 through January 17, 2018, authorities sent over 36,000 alerts⁵ to cell phones and radio and television stations. Ninety-six percent of the messages were weather alerts, 2

¹ *Executive Order No. 13407*, 71 Fed. Reg. 36975 – *Public Alert and Warning System* (June 26, 2006) directed the Secretary of the Department of Homeland Security (DHS) to enable secure delivery of coordinated messages to the American people through as many communication pathways as possible.

² IPAWS is also capable of sending national-level alerts from the President in the event of a national emergency. This function has only been used in a test scenario, including on October 3, 2018, but not in a real emergency.

³ The Executive Order also establishes the role of other federal agencies in the public alert system: the Federal Communications Commission oversees the emergency capabilities of communication systems; the Department of Commerce provides expertise regarding standards, technology, dissemination systems, and weather; and the Department of Defense ensures its functions are properly coordinated with the alert system.

⁴ For example, in the aftermath of the 2013 Boston marathon bombings, law enforcement issued an alert through IPAWS to city residents to "take shelter." During the August 2016 wildfires in San Luis Obispo, California emergency official sent alerts advising people to evacuate specific areas.

⁵ Alerting authorities also sent 9,564 test messages to radio and television stations.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

percent were child abduction alerts, and the remaining 2 percent were for various other reasons, such as evacuation orders and hazardous materials warnings. Appendix B provides more information on the alerting authorities and the alert types.

On January 13, 2018, the Hawaii Emergency Management Agency (HI-EMA), mistakenly issued an alert through IPAWS to individuals in Hawaii warning them of an inbound ballistic missile. The alert displayed on cell phones and was broadcast live on television and radio, resulting in widespread panic throughout Hawaii for 38 minutes, until HI-EMA sent out a notice that the alert was a false alarm. Senator Hirono of Hawaii requested the OIG examine FEMA's role in the transmission of the false missile alert. As part of our review, we interviewed FEMA and HI-EMA officials, and examined communications between the two agencies during the false missile alert. Additionally, we reviewed FEMA documents and reports, as well as public laws, rules and regulations.

Results of Inspection

After examining FEMA's current roles and responsibilities in the public alert and warning process, we concluded that FEMA has limited responsibility for the sending and canceling of state and local alerts. Following the Hawaii false missile alert, three U.S. Senators proposed legislation to define the federal government's role during false missile alerts, as well as to direct FEMA to recommend best practices in the alerting process.

During our review, we also identified two areas of concern regarding FEMA's overall oversight of IPAWS. Although FEMA maintains IPAWS as a messaging platform, state and local alerting authorities must obtain commercially-available emergency alert software to generate a message which passes through IPAWS for authentication and delivery. However, we found that FEMA does not require that this software perform functions critical to the alerting process, such as the ability to preview or cancel an alert. Instead, FEMA only recommends that software vendors include these capabilities as "best practices." FEMA also does not require that software vendors provide training to alerting authorities on how to use their chosen software. As a result, alerting authorities have experienced difficulties in various aspects of the alerting process.

FEMA Is Not Responsible for Sending or Canceling State and Local Alerts

In the aftermath of the Hawaii false missile alert, HI-EMA officials successfully canceled the alert, which prevented further dissemination, but were uncertain how to issue a false alarm. HI-EMA then contacted FEMA twice for assistance even though it was authorized to issue the false alarm without FEMA's approval. Ultimately, FEMA provided guidance to HI-EMA to correctly issue the



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

false alarm. FEMA provides overall support to the 1,030 alerting authorities on how to access and use IPAWS, and ensures IPAWS is operational at all times so that alerting authorities can rely on it to disseminate messages. FEMA officials stressed that state and local authorities are best able to determine alerting needs for a specific area.

HI-EMA Officials Successfully Prevented Further Dissemination of the Missile Alert but Were Uncertain How to Issue a False Alarm Message

Although HI-EMA officials knew the missile alert issued at 8:07am on January 13, 2018, was a mistake, they did not immediately issue a false alarm message. Instead, they canceled the alert at 8:12am, stopping further transmission to cell phones and on radio and television broadcasts, and then contacted FEMA for guidance. Based on FEMA’s guidance, HI-EMA issued the false alarm message at 8:45am. The following timeline details the Hawaii false missile alert on January 13, 2018, including HI-EMA’s interactions with FEMA:

Time	Event
8:05am	A night-shift supervisor decides to test incoming day-shift workers at HI-EMA with a spontaneous ballistic missile alert drill. The supervisor plays a recording over the phone that properly includes the drill language, “EXERCISE. EXERCISE. EXERCISE” at the beginning and end of the message, but also mistakenly includes the language “THIS IS NOT A DRILL.” The day-shift workers receive the recorded message on speakerphone. While other HI-EMA employees participating in the test understand that it is a drill, the employee at the alert origination terminal claims to believe it is not a drill.
8:07am	<p>The HI-EMA employee at the alert origination terminal generates an alert delivered through IPAWS to television and radio broadcasts and to cell phones. The cell phone message reads: “BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.”</p> <div data-bbox="574 1304 1024 1604" data-label="Image"> </div> <p>The radio and television message states, “The US Pacific Command has detected a missile threat to Hawaii. A missile may impact on land or sea within minutes. This is not a drill. If you are indoors, stay indoors. If you are outdoors, seek immediate shelter in a building. Remain indoors well away from windows. If you are driving, pull safely to the side of the road and seek shelter in a building or lay on the floor. We will announce when the threat has ended. This is not a drill. Take immediate action measures.”</p>
8:12am	HI-EMA cancels the alert, which ceases transmission of the alert over radio and television, and prevents additional cell phones (e.g., if a cell phone was not turned on at 8:07am or someone was out of cell coverage) from receiving the



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

	warning. At this time, HI-EMA does not send out another alert clarifying that the original message was a false alarm.
8:26am	HI-EMA attempts to contact FEMA but no one responds, and HI-EMA leaves message.
8:30am	HI-EMA makes second attempt to contact FEMA and reaches someone, who provides guidance on the correct procedures for issuing an all-clear, or false alarm, message.
8:45am	<p>HI-EMA generates an alert delivered through IPAWS to television and radio broadcasts and to cell phones. The cell phone message reads: “There is no missile threat or danger to the State of Hawaii. Repeat. False Alarm.”</p> <div data-bbox="574 558 971 793" data-label="Image"> </div> <p>The radio and television message states, “False Alert. There is no missile threat to Hawaii,” while the television crawler message reads, “False Alert. There is no missile threat or danger to the State of Hawaii. Repeat. There is no missile threat or danger to the State of Hawaii. False Alert.”</p>

As noted in the timeline above, FEMA provided guidance to the HI-EMA officials on how to correctly issue the false alarm.

FEMA Provides and Ensures Overall IPAWS Access but Is Not Responsible for Individual Alerts

While FEMA provides overall support to the 1,030 alerting authorities on how to access and use IPAWS, it does not play a major role in the actual sending or canceling of alerts. The IPAWS Program Management Office (PMO) may provide guidance and assistance but cannot review each alert to verify its accuracy. Alerting authorities, such as HI-EMA, are responsible for individual alerts and have the authority to send false alarm messages without FEMA’s approval. Proposed legislation in Congress may shift some of this responsibility to the Federal Government for missile alerts.

The Executive Order and later the Modernization Act, Pub. L. No. 114-143 (codified at 6 U.S.C. § 311 et seq.), direct FEMA to “consult, coordinate, and cooperate with...Federal, State, territorial, tribal and local governmental authorities.” Pub. L. No. 114-143 § 526(b)(7). To implement this directive, FEMA requires alerting authorities to sign a Memorandum of Agreement (MOA) with FEMA and obtain commercially-available emergency alert software from a list of FEMA’s pre-approved vendors.⁶ If the alerting authority needs to send a

⁶ FEMA requires that alerting authorities complete four steps in order to send alerts: 1) apply for a Memorandum of Agreement with FEMA; 2) select alert origination software that is compatible with IPAWS; 3) apply for public alerting permissions defining the types of alerts they intend to issue, as well as the geographic area of the alerts; and 4) complete web-based

www.oig.dhs.gov



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

warning or alert message, it uses the software to generate a message that complies with particular technological standards. The message then passes through IPAWS, which authenticates and delivers it through various public alerting systems.

FEMA's role in this process consists mainly of providing and maintaining the IPAWS messaging platform so that alerting authorities can rely on it to disseminate messages. The IPAWS PMO, consisting of 24 full-time Federal employees, oversees these aspects of IPAWS. However, FEMA officials we spoke to explained that alerting authorities, and not the PMO, are in control of sending and canceling alerts and warnings to their respective communities. They explained that while IPAWS logs every alert that comes through the system, PMO staff have no way of telling if any of these alerts is a mistake. For example, if an alerting authority meant to issue an alert for a flash flood warning but mistakenly issued one for a severe thunderstorm warning instead, only the alerting authority would know it was a false alert. The FEMA officials stated that PMO staff have no visibility into local emergencies and cannot verify alerting authorities' intent for each message transmitted through IPAWS.

One FEMA official explained that the alerting structure is based on the concept that the majority of emergencies "start local;" therefore, local officials are best able to provide timely, relevant, and accurate warnings. Because the PMO does not require alerting authorities to notify FEMA of alert mistakes, FEMA typically becomes aware of mistakes when the alerting authority contacts the PMO to request assistance with correcting them. FEMA does not officially track mistakes or alerting authority requests for assistance but, based on information FEMA provided to us, these situations are infrequent.

Regarding the Hawaii false missile alert specifically, three separate investigations or after-action reviews took place and reached similar conclusions. The Federal Communications Commission conducted an investigation, based on its oversight role of the emergency capabilities of communication systems, and determined that human error and inadequate management safeguards mainly contributed to the false missile alert. Hawaii charged a retired Brigadier General with conducting an investigation, which similarly concluded those factors at HI-EMA were the direct cause, and that FEMA played no role in the false alert. None of the state's findings were within FEMA's purview. Finally, FEMA conducted its own after-action review which stated, "HI-EMA possessed the authority to cancel or issue any follow-up information without intervention or approval from FEMA."⁷ In fact, FEMA requested via e-mail that a HI-EMA Deputy Chief amend previously disseminated language regarding the events of that day from:

training on how to access and use IPAWS. Information available at www.fema.gov/how-sign-ipaws (last visited September 13, 2018).

⁷ *Hawaii False Missile Alert After Action Report*, FEMA, March 30, 2018; obtained from FEMA on July 20, 2018.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

“After getting **authorization** from FEMA IPAWS, HI-EMA issued a “Civil Emergency Message” remotely by myself after building a template message.”

to:

“The FEMA IPAWS Team **assisted me with guidance** on sending a “Civil Emergency Message” (CEM) indicating “No Missile Threat or Danger to Hawaii”. The State of Hawaii Emergency Management Agency already is authorized to send CEM’s but requested advice prior to sending the alert.”

While the false alarm message was at the full discretion of HI-EMA, officials decided to delay sending the message until after HI-EMA employees contacted FEMA. We interviewed HI-EMA personnel who indicated that while they understood they did not need FEMA’s permission to send the false alarm message, they felt it prudent to seek advice and guidance on the appropriate message type because of the severity of the original alert. HI-EMA officials stated that, had they not been able to reach FEMA IPAWS representatives via phone, they would have eventually sent the false alarm message without further guidance. Moreover, the HI-EMA officials pointed out that IPAWS worked flawlessly during the false missile alert, in that it did exactly what the system is designed to do: disseminate an alert to a large number of people, in a specific geographic area, in a quick manner. Ultimately, the officials praised the IPAWS PMO for providing guidance during the false alert and for the cooperation and outreach they have received since the incident.

In the wake of the false alert, five Senators introduced the *Authenticating Local Emergencies and Real Threats (ALERT) Act* in February 2018, which calls for the Federal Government to be solely responsible for alerting the public of a missile threat. S. 2385, 115th Cong. § 7 (2018). The proposed legislation also aims to modify the Modernization Act by requiring FEMA to recommend best practices for procedures for state, tribal, and local government officials to authenticate civil emergencies and initiate, modify, and cancel alerts. *Id.* at § 3.

FEMA Does Not Require Vendors to Include Critical Functions or to Provide Training in Emergency Alerting Software

Although FEMA had no role in sending or canceling the Hawaii false missile alert, during our review we identified two areas of concern regarding FEMA’s oversight of IPAWS. First, FEMA does not require that software used by alerting authorities perform functions critical to the alerting process, such as the ability to preview or cancel an alert. Second, FEMA does not require that software vendors provide training to alerting authorities on how to use their chosen software. Until FEMA addresses these issues, the potential exists that alerting authorities will continue to experience problems during the alerting process.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Alerting authorities must choose and purchase commercially-available emergency alert software from a FEMA-approved vendor before they are able to send emergency alerts through IPAWS. As of July 2018, FEMA maintained a list of 23 vendors with emergency alert software approved to send IPAWS-compliant messages. Before approving a vendor, FEMA only requires the vendors to demonstrate the software's ability to author and send a properly formatted message through IPAWS. However, based on feedback from alerting authorities, FEMA determined that alerting authorities were unable to perform several "critical functions." Therefore, in a letter to vendors in February 2015, FEMA recommended that they ensure their software include these functions, such as the ability to preview or cancel an alert, the ability to alert the user when the software license had expired, and more intuitive user interfaces.⁸ According to FEMA officials, some vendors subsequently updated their software, but others did not. In response, in 2018, FEMA again sent a letter to vendors strongly encouraging them to ensure their software provided essential capabilities, which included ones in addition to those FEMA identified in 2015, such as the ability to send an alert to multiple channels and for users to see alert histories and logs.⁹

While the Hawaii false missile alert did not result from any of the concerns identified by FEMA, other examples demonstrate the need to include these capabilities in emergency alert software:

- The city of Monterey Park, CA, intended to send a test message, but inadvertently sent a live message. The emergency alert software did not include the ability to cancel the message.
- The state of Georgia intended to send an alert about a winter storm warning, but the message the public received was worded in a confusing manner and referenced a civil emergency, not a winter storm warning. The emergency alert software did not include the ability to cancel the message.
- A representative from the Pennsylvania Emergency Management Agency noted that the alerting software they purchased does not allow users to preview the actual message before sending.

FEMA has indicated that the critical functions it identified were not formal specifications, but a best practice tool. Until FEMA requires vendors to include these functions, alerting authorities may face continued challenges in various aspects of the alerting process.

⁸ 2015 FEMA Letter to Emergency Alerting Software Vendors, with the subject "Wireless Emergency Alerts, Origination Software Critical Functions" detailed minimum capabilities alerting software should possess.

⁹ 2018 FEMA Letter to Emergency Alerting Software Vendors, with the subject "Public Alert and Warning System (IPAWS) Alert Origination Software Critical Functions"



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

FEMA officials were also concerned that, due to a lack of training from the software vendors, alerting authorities experienced issues when sending or canceling alerts. The Modernization Act, Pub. L. No. 114-143 §526(b)(4)(B) directs FEMA to ensure that it conducts training for the public alert and warning system. FEMA fulfills that requirement by providing several online training opportunities specific to IPAWS, but it does not mandate vendors provide training to alerting authorities in their chosen emergency alert software. Similar to above, the lack of training was not a concern during the Hawaii false missile alert, as we confirmed that HI-EMA staff received adequate training from the vendor related to their chosen software. However, other examples highlight the need to ensure alerting authorities receive training regarding their specific software:

- In June 2017, Florida authorities attempted to send a child abduction alert (Amber Alert) to 54 separate locations (i.e., counties) but they were unaware the emergency alert software only allowed dissemination to a maximum of 31 locations at a time. Therefore, 23 locations that could have assisted in responding to the Amber Alert were not notified.
- During Hurricane Harvey in August 2017, two Texas counties relied on FEMA for assistance after they experienced problems sending alerts to the public. FEMA determined the errors resulted from a lack of training on the vendor software.

Nonexistent or inadequate system training for alerting authorities increases the potential for false or delayed alerts or cancellations, and other errors. Because each alerting authority can use one of multiple vendors to access the IPAWS interface, it is essential that they receive specific training and direction on their particular software.

Recommendations

To strengthen its oversight role, we recommend that the FEMA IPAWS PMO:

Recommendation 1: Require software vendors to include critical functions in their proprietary emergency alerting software that FEMA previously identified and communicated in 2015 and 2018.

Recommendation 2: Require software vendors to provide training on system functionality and capabilities to alerting authorities.

Management Comments and OIG Analysis

FEMA concurred with both report recommendations. Appendix A contains a copy of FEMA's management comments in their entirety. We also received one



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

technical comment from FEMA, and we incorporated that comment in the report where appropriate. We consider both recommendations to be resolved and open. A summary of FEMA's response and our analysis follows.

FEMA Response to Recommendation 1: FEMA concurred with the recommendation. The FEMA IPAWS PMO agreed to incorporate the functional requirements of the 2015 and 2018 vendor letters into an updated version of the MOA with FEMA that state, local, tribal, and territorial (SLTT) alerting authorities must enter into in order to leverage IPAWS services to send alerts and warnings to the public. The estimated completion date is October 31, 2019.

OIG Analysis: FEMA's proposed action is responsive to this recommendation. This recommendation is resolved and will remain open until we review documentation showing that FEMA incorporated the functional requirements of the 2015 and 2018 vendor letters into the MOA with SLTT alerting authorities.

FEMA Response to Recommendation 2: FEMA concurred with the recommendation. The FEMA IPAWS PMO agreed to incorporate a requirement for vendor-provided training into an updated version of the MOA with FEMA that SLTT alerting authorities must enter into in order to leverage IPAWS services to send alerts and warnings to the public. The estimated completion date is October 31, 2019.

OIG Analysis: FEMA's proposed action is responsive to this recommendation. This recommendation is resolved and will remain open until we review documentation showing that FEMA incorporated the requirement for vendor-provided training into the MOA with SLTT alerting authorities.

Objective, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

The objective of this review was to examine FEMA's role in the January 13, 2018 Hawaii false ballistic missile alert and to review whether FEMA exercises appropriate oversight of the use of the IPAWS.

To achieve our objective, we reviewed public laws, FEMA's IPAWS Program directives, policies and procedures, as well as investigations and after-action reports conducted as a result of the January 13, 2018, missile alert. We also interviewed officials from HI-EMA and FEMA's IPAWS PMO.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We conducted this review between April and July 2018 under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency.

The Office of Inspections and Evaluations major contributors to this report are Erika Lang, Chief Inspector; Amy Burns, Lead Inspector; Jennifer Berry, Senior Inspector; Samuel Tunstall, Inspector; and Michael Brooks, Independent Referencer.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
FEMA's Comments to the Draft Report

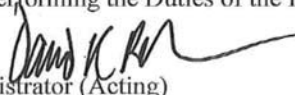
U.S. Department of Homeland Security
Washington, DC 20472



FEMA

October 26, 2018

MEMORANDUM FOR: John V. Kelly
Senior Official Performing the Duties of the Inspector General

FROM: David Bibo 
Associate Administrator (Acting)
Office of Policy and Program Analysis

SUBJECT: Management's Response to OIG Draft Report, "FEMA's
Oversight of the Integrated Public Alert and Warning System
(IPAWS)
(Project No. 18-073-ISP-FEMA)

Thank you for the opportunity to review and comment on the draft report. The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing the report.

FEMA is pleased with OIG's findings and remains committed to enhancing the effectiveness of the IPAWS Program Management Office (PMO).

The draft report contained two recommendations, with which FEMA concurs. Attached, please find our detailed response for each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were provided previously under separate cover. Please contact Gary McKeon, Director of FEMA's Audit Liaison Office, at 202-646-1308 with any questions or concerns. We look forward to working with you in the future.

Attachment

www.fema.gov



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**Attachment: FEMA Management Response to Recommendations Contained in
Project No. 18-073-ISP-FEMA**

The OIG recommended that the FEMA IPAWS PMO:

Recommendation 1: Require software vendors to include critical functions in their proprietary emergency alerting software that FEMA previously identified and communicated in 2015 and 2018.

Response: Concur. The FEMA IPAWS PMO intends to incorporate the functional requirements of the 2015 and 2018 vendor letters into an updated version of the Memorandum of Agreement (MOA) with FEMA that state, local, tribal, and territorial (SLTT) alerting authorities must enter into in order to leverage IPAWS services to send alerts and warnings to the public. Each MOA expires and must be renewed every three years. Incorporating the functional requirements into the MOA will ensure that SLTT alerting authorities utilize alerting software with critical functions identified by FEMA.

Estimated Completion Date (ECD): October 31, 2019

Recommendation 2: Require software vendors to provide training on system functionality and capabilities to alerting authorities.

Response: Concur. The FEMA IPAWS PMO intends to incorporate a requirement for vendor-provided training into an updated version of the MOA with FEMA that SLTT alerting authorities must enter into in order to leverage IPAWS services to send alerts and warnings to the public. This requirement will ensure that SLTTs obtain training from their respective alerting software vendors necessary to maintain proficiency on system functionality and capabilities.

ECD: October 31, 2019



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Alerting Authorities and Types of Alerts

As of February 2018, over 1,030 alerting authorities had access to IPAWS. Table 1 describes the various types and number of alerting authorities.

Table 1: Type and Number of Alerting Authorities, as of February 2018

Type of Alerting Authority	Number of Alerting Authorities
Local	950
State	72
Territory	3
Tribal	3
Federal*	2
TOTAL	1,030

Source: OIG analysis of FEMA data

* Two Federal agencies are considered alerting authorities for local emergencies: the National Center for Missing and Exploited Children for child abduction alerts and the National Weather Service for weather alerts.

From April 2012 through January 17, 2018, these alerting authorities sent over 34,000 alerts to cell phones. Ninety-six percent of these messages were weather alerts, 2 percent were child abduction alerts, and the remaining 2 percent were for other various reasons. Table 2 describes the type and number of alerts sent to cell phones.

Table 2: Emergency Alerts sent to Cell Phones

Type of Event	Event Description	Number of Alerts
Weather	Flash flood warning	21,127
Weather	Tornado warning	11,221
Child abduction	Child abduction emergency	697
Weather	Hurricane warning	369
Weather	Blizzard	302
Other	Local area emergency	296
Weather	Dust storm warning	258
Other	Civil emergency message	198
Other	Law enforcement warning	73
Weather	Severe thunderstorm warning	70
Weather	Winter storm warning	61
Other	Fire warning	60
Other	Evacuation Immediate	45
Weather	Flood warning	23
Other	Civil danger warning	19
Other	Shelter in place warning	14
Other	Hazardous materials warning	11
Weather	Tsunami warning	1
TOTAL		34,845

Source: OIG analysis of FEMA data



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

During the same time period, alerting authorities sent over 10,000 alerts to radio or television stations. The vast majority (92 percent) were tests of the alerting system.

Table 3: Emergency Alerts sent to Radio and Television Stations

Test emergency alerts sent to radio or television stations	9,564
Non-test emergency alerts sent to radio or television stations	858
Total emergency alerts sent to radio or television stations	10,422

Source: OIG analysis of FEMA data



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
FEMA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees
Senator Mazie Hirono

External

Hawaii Emergency Management Agency

Additional Information and Copies

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.



OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305