OCIO Office of the DOT Chief Information Officer

U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration
Office of Security and Hazardous Materials Safety (ASH)
Emergency Notification System (ENS)

Responsible Official

Lisa Lefler
Division Manager
ens-support@faa.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2019.02.28 15:10:08 -05'00'

Executive Summary

Federal Aviation Administration's (FAA) Emergency Notification System (ENS) uses the AtHoc Network Communication Suite (AtHoc Suite) to provide alert notifications during all hazards, threats, and emergencies to FAA employees[1] and contractors. Other federal agencies, tenant organizations in FAA facilities, non-FAA students at the FAA Academy, and certain state/local agencies (hereinafter referred to as external recipients) may also opt to receive alert notifications from the FAA. ENS uses AtHoc Suite, a cloud-based service operated by AtHoc, a division of Blackberry, which provides the ability to send alert notifications, and in some circumstances, receive responses via an internet connection. ENS is administered and maintained by the FAA's Office of Security and Hazardous Materials Safety (ASH), National Security Programs and Incident Response, Command and Control Communications Division (AXE-400). This Privacy Impact Assessment was developed in accordance with Section 208 of the E-Government Act of 2002, because the FAA collects personally from members of the public in order to provide them alerts via ENS.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[2]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk*
- *Accountability for privacy issues*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

[1] For purposes of the PIA exclusively, "employee" includes interns or students.

[2] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo M-03-22 dated September 26, 2003).

Introduction & System Overview

Title 49 of United States Code gives the Federal Aviation Administration (FAA) the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating U.S. commercial space transportation.

Background

Incidents such as Hurricane Katrina in 2005; the 2011 Washington, DC-area earthquake; the 2012 William J. Hughes Technical Center (WJHTC) fire; the 2013 Boston Marathon bombing; and the 2014 Chicago Air Route Traffic Control Center fire, along with various emergency exercises, highlighted the need to improve the FAA's ability to communicate with and account for the status of employees and contractors in emergency situations. It was determined that the Washington Operation Center (WOC) and the Regional Operation Centers (ROCs) were working to replace EMERGIN, an existing emergency notification system had reached its end-of-life cycle and was no longer supported. A new emergency notification system was needed to support their business function of sending alert notifications regarding events in the National Airspace System (NAS) to FAA executives and other designated personnel. The workgroup recommended to the Business Council that the agency leverage the work initiated by the WOC and ROC and obtain an emergency notification system capable of supporting the entire FAA. This enterprise emergency notification system will give the FAA a single, uniform, and comprehensive alert notification capability for use by all FAA organizations.

Emergency Notification System (ENS) Overview

The Office of Security and Hazardous Materials Safety (ASH), Office of National Security Programs and Incident Response, Command and Control Communications Division (AXE-400) replaced EMERGIN, referred to in this document as "the legacy system" with the Emergency Notification System (ENS). This was done to facilitate the delivery of emergency and other alert notifications. The ENS messaging platform sends alert notifications through several communication pathways, including voice[3], email, text, the AtHoc desktop client application[4] and/or AtHoc mobile application.

ENS provides a secure and easy-to-use platform to:

- Provide situational awareness to appropriate personnel;
- Obtain information about personnel status per Human Resources Policy Manual, Chapter 11.4, Accounting for Federal Aviation Administration Employees in Emergencies;
- Send voice, email, text, desktop and/or mobile notifications;
- View historical and current alerts; and

[3] AtHoc uses voice call notifications over the Internet or a telephone network to initiate and end voice calls. This service provides the "dial tone" to commercial phone carriers to enable AtHoc to deliver notifications via phone calls, play voice messages , interact with recipients, detect voice answering services and answer call backs from users who received a voice message.

[4] The AtHoc desktop notification client application is a lightweight Windows or Mac OS X application used to deliver notifications to users' desktops and capture their responses. The desktop notification user experience is in the form of always-on-top popup windows, which allows the users to select a response (i.e., (1) I'm okay, (2) I need help) before dismissing the popup notification. This client application is installed on FAA workstations/laptops ONLY.

- Publish and manage alerts.

Types of alert notifications discussed in Appendix A include but are not limited to:

- Weather alerts (such as tornados);
- Man-made threats/events (such as threats against aircraft or FAA/aircraft personnel, disruptive passengers on aircraft, intoxicated air crew member, active shooter at an FAA facility);
- Technological threats (such as laser strikes, or drone events);
- Physical and environmental hazards (such as a gas leak on an FAA facility); and
- Medical incidents (such as a medical emergency on an aircraft or in an FAA facility).

ENS User Roles

Operators - Operators who are FAA employees and contractors are designated by their organization to use ENS to send emergency and other alert notifications. Operators must successfully complete ENS training prior to being granted system permissions. Operators are assigned to one of the following three (3) system-defined roles:

- Alert Publisher/Advanced Alert Manager (AP/AAM) - Send, monitor, track, and cancel active alert notifications;
- Organization Administrator (OA) - Assign permissions to APs/AAMs within their respective organization; and
- Enterprise Administrator (EA) - Operate and maintain the application, assign permissions to OAs, function as an OA and an AP/AAM.

End Users - End users consist of FAA personnel including contractors, and external recipients. End users may receive alert notifications via voice, email, text, desktop and/or mobile notifications. End user enrollment process is as follows.

FAA Employees and Contractors

Contact information for FAA employees and contractors is automatically ingested from FAA MyProfile to ENS. MyProfile provides ENS with employees' and contractors' full names, work emails, office locations, region codes, routing codes, work phone numbers and FAA-issued mobile device numbers. MyProfile also provides geographic location and region information. This is used to separate users into one of the defined geographic partitions in the ENS: East, Central, West, and OCONUS. This allows the individual to receive alert notifications of pertinent emergency events that occur within their specific region or geographic location. ENS also ingests personal mobile numbers and personal email addresses if the FAA employee or contractor has opted to provide that information in MyProfile. ENS synchronizes with FAA MyProfile through a daily data pull. This helps to ensure that the contact information used by ENS is current.

External Recipients

External recipients may be enrolled to receive alert notifications by using the AtHoc Connect service or by requesting the FAA to enroll the external recipient as an end-user.

External recipients who are registered with AtHoc will send a request to the FAA through the AtHoc Connect service requesting to receive alert notifications. In doing so the FAA will receive a request with the organization's name, organization's address, organization's description, the organization's point of contact name, official email address and official phone number of the point of contact. External recipients that are users of AtHoc Connect service are responsible for maintaining their contact information current in the AtHoc directory.

External recipients that opt to enroll as an end-user will provide the FAA with their organization's name, organization's address, organization's description, the organization's point of contact name, official email address, official phone number of the point of contact, and categories of alert notifications. This information is manually entered into ENS through the AtHoc web interface, https://alerts6.athoc.com. Routinely the FAA will sends periodic reminders to external recipients for updates to their organization's contact information to maintain the information current in ENS.

Sending Alerts through ENS

Typically, ENS uses AtHoc to send alert notifications related to incidents such as a commercial power outage at an airport, a laser strike on a police helicopter, a temporary loss of communication with a military aircraft, or temporary flight delays due to extreme weather conditions. To do this, AtHoc sends alert notifications by selecting a pre-defined distribution list, consisting of contact information that was provided during the registration or enrollment process. The Operator log-ins to the ENS using their FAA-issued Personal Identity Verification (PIV) card and creates an alert notification. The Operator then creates a message that includes a description of the incident and the date, time, and location. The message may include the aircraft registration number when an Operator deems it necessary to identify the aircraft in response to or in preparation for an emergency situation. However, in most instances, this kind of identifying information is not incorporated. A conference bridge number may be included in the content of the message to allow additional communication about the incident, if necessary. For additional information regarding system usage see Appendix A.

The AtHoc Mobile Application

ENS supports the use of the AtHoc mobile application, which is a free application for the iOS and Android mobile devices. This mobile application allows Operators to send alerts and end-users to receive and respond to alerts. Operators and end-users who voluntarily choose to download the AtHoc mobile application for the iOS or Android mobile devices must first fulfill the registration requirements from the respective app stores. Once the mobile application is downloaded and installed, the Operator or end user must launch the AtHoc mobile application, set permissions to allow their mobile device to receive alert notifications, and follow the steps below to link their account to the mobile application.

1. The Operator or end-user will enter their work email address and submit the registration request. A verification email is sent to the email address provided that includes an organization code.
2. Upon receipt of the email, the Operator or end-user selects the "Verify Now" prompt included in the verification email and enter the provided organization code.
3. Once ENS confirms that the organization code is valid, the Operator or end-user will receive a registration confirmation message..

Also during the registration process, a unique identifier for the mobile application is established and sent to AtHoc. This identifier establishes the authorization and access between AtHoc and the AtHoc mobile application. This identifier is associated with the individual's organization and email address and assigned ENS role (Operator or end user – it is not associated with any other personal identifier. No additional information is exchanged between the AtHoc mobile application and ENS during the registration process.

Once registration is complete, the mobile application prompts the Operator or end-user to enable the location services feature. This allows the mobile application to receive ENS alerts that are relevant to the mobile device's physical location. The mobile application uses no additional features of the iOS and/or Android mobile device.

Operators that use the AtHoc mobile application must enter their password to access the mobile application alert publishing feature and to create and send alert messages. AtHoc mobile application does not support the use of a PIV card to access the mobile application through a mobile device; however, Operators may only send notifications from FAA government-issued mobile devices. AtHoc implements secure communication between the mobile application and AtHoc using the HyperText Transfer Protocol Secure (HTTPS) protocol. Contact information provided by FAA employees, contractors or other entities is not accessible through the mobile application. The mobile application accesses only distribution lists defined in the ENS web interface.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[5], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[6].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Records in ENS may be retrieved by an individual's name, the date of the incident, or the alert notification type. However, ENS is not the point of collection for this information. FAA employees' and contractors' information is obtained from MyProfile and in accordance with, and as required, a System of Records notice which discusses the Department's privacy practices. A Privacy Act statement explaining the collection, use, sharing, maintenance and disposal of PII is provided at the initial point of collection. The FAA protects records subject to the Privacy Act in accordance with the Department's Published System of Record Notice (SORN) entitled DOT/ALL 22, Emergency Contact Records (ECR) -- Not Covered by Notices of Other Agencies, November 9, 2010 75 FR 68852 With respect to information on individuals external to the FAA, notice and any opportunity to consent will be provided by their respective organizations.

The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into the ENS.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

ENS pulls contact information for FAA employees and contractors from MyProfile. This includes FAA employees' and contractors' name, work email address, office location, routing code, office phone number, FAA issued mobile device number and region code. FAA employees and contractors are responsible for the accuracy of their information. If corrections are required, an employee or contractor must access MyProfile to make the necessary changes to their profile. ENS synchronizes new profiles or changes to a user's profile through a daily data pull from MyProfile. This ensures that FAA employees' and contractors' contact information is current in ENS, to the extent the data in MyProfile is current. For an FAA employee's or contractor's contact information to be removed from ENS, MyProfile must send the system a delete change status for the individual. A delete change status triggers a

[5] https://cio.gov/wp-content/uploads/downloads/2012/09/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[6] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

delete action in ENS to remove the employee or contractor's profile. A delete change status indicates the individual has separated from the Agency.

External recipient organizations registered with AtHoc Connect are responsible for updating and managing their employees' contact information as part of the inter-organization communication processes within the AtHoc Connect directory. This is also true of individuals who are registered with AtHoc Connect. External entities or individuals who are unable to use the AtHoc Connect service provide contact information, including any updates or amendments, to an FAA EA or OA to be entered manually. FAA EA or OA Operators also have the ability to disenroll or disable external recipients.

The ENS system uses contact information to send alert notifications of real-time crises or emergencies. Alert notifications do not contain PII in the body of the message, barring certain circumstances, where an Operator may deem it necessary to include an aircraft registration number and pilot's name in response to or in preparation for an emergency situation.

Under the provisions of the Privacy Act, individuals may request searches to determine if any records which pertain to them have been added to ENS. Individuals inquiring whether their records appear in this system must inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington, DC 20591

The following must be included in all requests:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records

Contesting record procedures:

Individuals contesting information about them that is contained in this system should make their requests in writing, detailing the reasons why the records should be corrected, to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington, DC 20591

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

ENS data will be used by the FAA consistent with the purposes for which it was collected, as described in the DOT/ALL 22, Emergency Contact Records (ECR) -- Not Covered by Notices of Other Agencies, Emergency November 9, 2010 75 FR 68852. For FAA employees and contractors, the contact information is used to send alert notifications. If the individual has provided his or her personal email address and personal cell phone number in the MyProfile, that information may also be used for the purpose of sending alert notifications to registered personnel of real-time crises or emergencies. For external recipients, the system collects only business information. For emergencies involving aircraft, the aircraft registration number may be included in the in the body of the message when an Operator deems it necessary to identify the aircraft in response to or in preparation for an emergency situation.

DOT/ALL 22 is the official system of records notice of contact records that are used by DOT human resources specialists; security, safety, and emergency response coordinators; members of emergency response teams and other work units; and supervisors and administrative assistants, on a need to know basis, for reasons such as the following:

- To identify and locate emergency personnel to work during emergencies, office dismissal, or closure situations;
- To identify and locate mission critical emergency personnel to participate in continuity of operations exercises and to provide continuity of operations during national security, natural disaster, pandemic flu, and similar situations;
- To account for and maintain communication with personnel during an office closure, building evacuation, natural disaster, pandemic flu, or other office emergency (e.g., to make telework or leave arrangements), or to contact them about an urgent work matter (e.g., during off-duty hours);
- To notify designated third-party contact(s), to help locate a personnel member who is absent without leave, or to assist a personnel member in an evacuation or if he or she is injured, ill or incapacitated at work; and
- To deliver an identical automated message to all of the component's or office's personnel, alerting them to conditions such as power outages, road closings, and extreme weather.
- The FAA is charged with providing and maintaining situational awareness to affected personnel of real-time crises or emergencies and accounting for personnel status and their safety. The ENS operates under, the following authorities:
  - The National Security Act of 1947, as amended;
  - The Homeland Security Act of 2002 (Pub. L. 107–296), dated November 25, 2002;
  - Executive Order 12148, Federal Emergency Management, dated July 20, 1979, as amended;
  - Executive Order 12656, Assignment of Emergency Preparedness responsibilities, dated November 18, 1988, as amended; and
  - Executive Order 13286, Establishing the Office of Homeland Security, dated February 28, 2003.

Data Minimization & Retention

DOT will collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT will retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The FAA collects the minimum amount of information necessary to contact individuals during emergency situations. ENS records will be maintained in accordance with National Archives and Record Administration (NARA) approved records disposition schedule DAA-GRS-2016-0004, GRS 5.3, Item 020; Employee Emergency Contact Information:

Contact records are destroyed when superseded or obsolete, or upon separation or transfer of employee.

Employee directories that contain information about where employees are located in facilities and work phone numbers will be maintained in accordance with DAA-GRS-0012-0002, GRS 5.5, Item 20 ; Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use. Alert received by the mobile application will be purged within 48 hours of the alert ending. Alerts published by the mobile application will be maintained in accordance with approved NARA schedule.

Use Limitation

DOT will limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

FAA uses and shares information to provide alert notifications during all hazards, threats, and emergencies to FAA employees, contractors, and external recipients. External recipients include other federal agencies, tenant organizations in FAA facilities, non-FAA students at the FAA Academy, and certain state/local agencies who have opted to receive alert notifications from the FAA. Privacy Act records collected, used, and maintained by ENS are shared in accordance with the Department's system of records notice DOT/ALL 22, Emergency Contact Records (ECR) -- Not Covered by Notices of Other Agencies, November 9, 2010 75 FR 68852. In addition to other disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

- DOT may share contact information about emergency personnel and mission critical emergency personnel who are assigned to DOT emergency-related programs with Federal, State and local governmental agencies or executive offices, relief agencies, tax-exempt non-profit organizations, and nongovernmental organizations, when disclosure is appropriate for proper coordination of security, protective, and other official operations and functions in response to or in preparation for emergency situations.

The Department has also published 14 additional routine uses applicable to all DOT Privacy Act systems of records, including this system. The routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010 and 77 FR 42796, Jul 20, 2012, under "Prefatory Statement of General Routine Uses" available at https://www.transportation.gov/privacy.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

The ENS pulls FAA personnel data from MyProfile and synchronizes the data daily to maintain accurate, complete, and timely contact information. FAA staff is ultimately responsible for the accuracy of information they provide and maintain within MyProfile.

External recipient organizations registered with AtHoc Connect are responsible for updating and managing their employees' contact information as part of the inter-organization communication processes within the AtHoc Connect directory. This is also true of individuals who are registered with AtHoc Connect. External entities or individuals who are unable to use the AtHoc Connect service provide contact information, including any updates or amendments, to an FAA EA or OA to be entered manually. FAA EA or OA Operators also have the ability to disenroll or disable external recipients.

AtHoc has validation rules in place that govern the structure of email address and phone numbers to increase the likelihood that ENS will contain accurate contact information. An example would be a missing punctuation such as ".com" or "@" or missing a digit to a phone number.

Security

DOT will implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006; and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

The Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessment Organization performed a security assessment of security controls for AtHoc Suite that includes the AtHoc mobile application. The security assessment included vulnerability testing and penetration testing.

The ENS was issued a three year authority to operate (ATO) on February 15, 2017. Additionally, AtHoc Suite which includes the AtHoc mobile application received an approved cloud authorization from the FedRAMP on March 10, 2017 for the AtHoc cloud services leveraged by the ENS.

Access to the ENS is implemented based on the principle of least privilege and limited to individuals with appropriate security credentials, an authorized purpose, and need-to-know. FAA personnel with authorization to logon to the ENS web interface use the PIV card for two factor authentication before granting access.

Accountability and Auditing

DOT will implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FAA Order 1370.121 implements the various privacy requirements based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347,) the FISMA, DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, additional policies and procedures related to the access, protection, retention, and destruction of PII are consistently applied. Federal employees and contractors are given clear guidance in their duties as related to collecting, using, and processing privacy data in the form of mandatory annual security and privacy awareness training, as well as the implementation of FAA Order 1370.121. The FAA will conduct periodic privacy compliance reviews of the ENS as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Lisa Lefler
Division Manager
Command and Control Communications (AXE-400)

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer

Appendix A

The types of notifications that an ENS Operator may send as alerts include, but are not limited to, weather and building closures; security incidents (e.g., active shooter), and environmental hazards (e.g., gas leak) at or affecting FAA facilities; unruly passengers on aircraft; laser strikes, unmanned aircraft system accident or event); manned aircraft accident or event; medical emergencies of persons on aircraft; and reports of threats against aircraft or FAA personnel, etc.

Weather related delays and closures are common occurrences that requires providing an alert notification to FAA employees and contractors impacted by the delay or closure. In this event, an ENS Operator, logs into the ENS via the URL https://alerts6.athoc.com and selects an appropriate alert template to create an alert message adding only the details of the delay or closure. The following is an example of the message, which does not include any PII:

"The AWA (Washington Capital Region) Regional Office will be CLOSED today <<02/10/2017>> due to current and forecasted weather conditions. Telework and emergency designated employees should follow existing personnel policies. Visit http://my.faa.gov/go/status for additional information."

The ENS Operator then publishes and disseminates the alert notification to FAA employees and contractors voice, email, text, desktop and/or mobile notifications. Messages sent via email include the recipient's email address in the recipients field (i.e., "to:") and the alert notification content in the body of the email. Alert notifications sent by text include the recipient's mobile phone number in the recipients field (i.e., "to:") and the alert notification content in the body of the text message. Alert notifications sent via the mobile application only include the alert notification message.

Responding to an alert

The ENS Operator, through the alert notification, may solicit a response from the recipient to account for the FAA staff member's safety. The recipient selects the appropriate response option from the alert notification and responds by replying with the digit associated with the response option, for example:

1. I am ok
2. I need assistance, connect me to the Emergency Hotline
3. Not in the Area