U.S. Department of Transportation

# Privacy Impact Assessment
# Federal Aviation Administration (FAA) Security & Hazardous Material Safety (ASH) Emergency Notification System (ENS)

## Responsible Official

Kevin VanHaren
ens-support@faa.gov

## Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

## Executive Summary

The FAA's Office of Security and Hazardous Materials Safety (ASH) Federal Aviation Administration (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 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 operates under the following authorities: Public Law 93-366; Public Law 112-95 Section 3337; 49 United States Code (U.S.C.) 401018; 49 U.S.C. 401039; National Communications System Directive (NCSD) 3-1010, Minimum Requirements for Continuity Communications Capabilities; National Security Presidential Directive (NSPD) 5111 and Homeland Security Presidential Directive (HSPD) 2012: National Continuity Policy Federal Continuity Directive (FCD) 113 and FCD 21.

The FAA is publishing this Privacy Impact Assessment (PIA) for ENS in accordance with Section 208 of the E-Government Act of 2002 because the system processes Personally Identifiable Information (PII) from members of the public, including non-FAA Federal, state, and local government employees/contractors who receive FAA emergency and non-emergency notifications.

## 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.*[1]

*Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protecting the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's*

[1] 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 of M-03-22 dated September 26, 2003).

*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; and*
- *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.*

## Introduction & System Overview

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 FAA 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, as the then-existing emergency notification system 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.

***Emergency Notification System (ENS) Overview***

The ASH, Office of National Security Programs and Incident Response, Command and Control Communications Division (AXE-400) replaced the old FAA system, EMERGIN, 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, email, text, the AtHoc desktop client application, 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
- Publish and manage alerts.

Types of alert notifications discussed 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 aircrew 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, and function as an OA and an AP/AAM.

End Users - End users consist of FAA personnel including contractors, and non-FAA Federal, state, and local government employees/contractors who receive emergency and non-emergency notifications. End users may receive alert notifications via voice, email, text, desktop, and/or mobile notifications. The end user enrollment process is as follows.

***FAA Employees and Contractors Recipients***

Contact information for FAA employees and contractors is automatically ingested from the FAA system MyProfile to ENS. MyProfile provides ENS with the employee and contractor's full name, work email, office location, region code, routing code, work phone number, and FAA-issued mobile device number. 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.[2] 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 exchange. 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[3] or by requesting for the FAA to enroll the external recipient as an end-user. External recipients who are registered with AtHoc send a request to the FAA through the AtHoc Connect service requesting to receive alert notifications. In doing so the FAA receives a request with the organization’s name, address, description and point of contact (POC) name, POC official email address, and POC official phone number. 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 end-user provide the FAA with their organization’s name, organization’s address, organization’s description, the organization POC name, official email address, official phone number of the POC, and categories of alert notifications. This information is manually entered into ENS by FAA program personnel through the AtHoc web interface. The FAA sends periodic reminders via email to external recipients requesting updates to their organization’s contact information to ensure the information in ENS remains current.

### Sending Alerts through ENS

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, an FAA operator or FAA employee designated by their organization to use ENS to send emergency and other alert notifications, logs into 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. In most instances, this kind of identifying information is not incorporated. AtHoc sends the alert notification by selecting a pre-defined distribution list, consisting of contact

[2] OCONUS means outside the contiguous United States, which includes Alaska, Hawaii, and US territories and possessions, such as Puerto Rico.

[3] AtHoc Connect is a cloud-based service operated by AtHoc, a division of Blackberry, which is an integrated collection of four component applications, all compliantly secured with behind firewall technology used for network crisis communication.

information that was provided by the individual during the registration or enrollment process. A conference bridge number may be included in the content of the message to allow additional communication about the incident, if necessary.

### The AtHoc Mobile Application

ENS supports the use of the AtHoc mobile application, which is a free application for Apple iOS[4] 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 enters their work email address and submits 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 enters the provided organization code.
3. Once ENS confirms that the organization code is valid, the operator or end-user receives 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

[4] iOS means iPhone operating system.

government-issued mobile devices. AtHoc implements secure communication between the mobile application and AtHoc using the Hyper Text 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 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 risks. 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.*

ENS is a privacy-sensitive system because it maintains collects, uses, disseminates, and retains PII from non-FAA Federal, state, and local government employees/contractors to receive emergency and non-emergency notifications. Policies, procedures, and practices for information storage, data use, access, notification, retention, and disposal are described herein in this PIA.

The FAA protects records subject to the Privacy Act in accordance with the following Department's Published System of Records Notices (SORNs):

DOT/ALL 22, *Emergency Contact Records* (ECR) Not Covered by Notices of Other Agencies, 75 FR 68852 (November 9, 2010) covers contact information records about DOT employees/contractors who receive emergency and non-emergency notifications. The records include full name, business email address, business phone number (cell phone and desk phone, and airplane tail number not collected, but may be included in

[5] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[6] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

the incident/ accident alert notification). The records may also include the following PII about DOT personnel including full name, FAA/personal email address, FAA location/address, telework zip code, FAA/personal phone number (cell and desk phone), username, organization name, and Internet Protocol (IP) address, which is masked.

DOT/ALL 16, *Mailing Management System*, 71 FR 35319 (June 19, 2006) covers non-FAA/DOT employee and contractor information collected directly from individuals. The records may include the following PII about DOT personnel: full name, business/.gov email address, business location/address, business phone number (cellphone and desk phone), and airplane tail number (not collected, but may be included in the incident/accident alert notifications).

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency in the ENS system.

## 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 the FAA employee and contractor 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 employee's and contractor's 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 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 can also dis-enroll 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, such as 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 of the ENS system to determine if any records have been added that may pertain to them and if such records are accurate.

For all inquiries related to the information contained in the ENS, the individual may appear in person, send a request via email (privacy@faa.gov), or in writing to:

Federal Aviation Administration

Privacy Office

800 Independence Avenue, SW

Washington, DC 20591

The request must include the following information:

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

Contesting record procedures:

Individuals wanting to contest information about themselves 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

If you have comments, or concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

## 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.*

Congress has authorized the FAA Administrator to develop systems and/or tools to support sending emergency and non-emergency notifications to subscribed users ENS addresses the unique demands of the FAA's workforce and operates under the following authorities:

- Public Law 93-366
- Public Law 112-95 Section 3337
- 49 U.S.C. 401018
- 49 U.S.C. 401039
- NCSD 3-1010, Minimum Requirements for Continuity Communications Capabilities
- NSPD 5111 and HSPD 2012: National Continuity Policy
- FCD 113 and FCD 21

ENS collects PII for the following purposes:

- ENS system access and program management
    - From FAA employees and contractors: Full name, FAA email address, FAA phone number.
- For emergency and non-emergency notifications
    - From members of the public including other Federal, state, and local government employees/contractors who receive emergency and non-emergency notifications from the FAA: Name, business email address, and business phone number.

ENS uses this information in accordance with the purposes for which it is collected under the following SORNs:

DOT/ALL 22, *Emergency Contact Records* (ECR) Not Covered by Notices of Other Agencies, 75 FR 68852 (November 9, 2010) covers contact records of individuals who are DOT employees/contractors.

DOT/ALL 16, *Mailing Management System*, 71 FR 35319 (June 19, 2006) covers records of individuals who are not DOT employee/contractor individuals.

## Data Minimization & Retention

*DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.*

The FAA collects the minimum amount of information from individuals to support FAA's Emergency Notification. The FAA maintains different types of records in accordance with the following National Archives and Record Administration (NARA) approved General Retention Schedules[7] (GRS):

- The FAA collects the minimum amount of information necessary to contact individuals during emergency situations. ENS records will be maintained in accordance with NARA GRS 5.3, Item 020, DAA-GRS-2016-0004; Employee Emergency Contact Information:
    - Contact records are destroyed when superseded or obsolete, or upon separation or transfer of employee.
- Some records in ENS are transitory and intermediary records. Transitory records are records of short-term value (generally less than 180 days). Intermediary records are those involved in creating a subsequent record. These records do not document significant decisions or actions an agency takes. These records are maintained in accordance with approved NARA GRS 5.2.
    - Transitory records are temporary and should be destroyed when no longer needed for business use, or according to an agency predetermined time period or business rule. DAA-GRS-2022-0009-0001.
    - Intermediary records are temporary and should be destroyed upon creation or update of the final record, or when no longer needed for business use, whichever is later. DAA-GRS-2022-0009-0002.
- Individual's system access and audit log records are maintained in the system as temporary records and are destroyed when business use ceases. The applicable records retention schedule is NARA GRS 3.2, approved September 2014, *Information Systems Security Records*, Item 30, DAA-GRS-2013-0006-0003.

## Use Limitation

*DOT shall 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.*

[7] General retention schedules are used by the FAA to determine how long to maintain an individual's records and/or when to delete the individual's records and in order to promote consistent retention practices.

The PII in ENS is used for emergency notifications and access and authentication to the system. The FAA does not use the PII for any other purpose.

The FAA/DOT limits the scope of PII collected in ENS to support the purpose specified in SORNs DOT/ALL 22, Emergency Contact Records (ECR), Not Covered by Notices of Other Agencies, November 9, 2010 75 FR 68852, which covers DOT employees/contractors and DOT/ALL 16, Mailing Management System, 71 FR 35319 (June 19, 2006), which covers records of individuals who are not DOT employee/contractor individuals. FAA/DOT may not share personal information.

The Department has also published 17 additional routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019, under "Prefatory Statement of General Routine Uses."

## 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).*

ENS collects, uses, and retains data that is relevant and necessary for the purpose for which it was collected. 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. The FAA promotes data quality by encouraging individuals to keep their information current. Users are reminded via Electronic Learning Management System (eLMS) SAVI to maintain their MyProfile including their required trainings.

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 can also dis-enroll or disable external recipients. The PII is collected directly from the individual and thus is assumed to be accurate.

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 shall 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 the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the ENS system to test security processes, procedures and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to know are authorized to access the records in ENS. All data in-transit is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessment to test and validate security process, procedures and posture of the system. Based on the security testing and evaluation in accordance with the FISMA, the FAA issues ENS an on-going authorization to operate.

## Accountability and Auditing

*DOT shall 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 1370.121B, *"FAA Information Security and Privacy Program & Policy,"* implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

DOT implements 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.

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with ENS are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of ENS as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

## Responsible Official

Kevin VanHaren

System Owner

Program Manager, ASH

## Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer