U.S. Department of Transportation

Privacy Impact Assessment (PIA)

Federal Aviation Administration (FAA)
Office of Security and Hazardous Materials Safety (ASH)
Emergency Operations Network (EON)

Responsible Official
Kevin Van Haren
c3techdesk@faa.gov

Reviewing Official
Karyn Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

May 23, 2002

Executive Summary

The Federal Aviation Administration (FAA) Office of Security and Hazardous Materials Safety (ASH) Emergency Operations Network (EON) is a set of integrated web-based emergency operations and information sharing tools used to collect and provide real-time notification of National Airspace System (NAS) incidents and accidents via email or mobile phone through the Emergency Notification System (ENS) to FAA employees and contractors, federal officials, interagency security partners, and other members of the aviation community to ensure the safety and security of the national airspace.

The FAA is publishing this Privacy Impact Assessment (PIA) for the EON pursuant to Section 208 of the E-Government Act of 2002 because this application collects and stores personally identifiable information (PII) from members of the public, such as pilots, law enforcement, and others in the aviation community.

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 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; and*

[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).

- *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

In August 1974, in response to a surge in aircraft hijackings, Public Law 93-366 established the exclusive statutory role of the FAA in aviation security and created the Office of Civil Aviation Security (ACS). Following the reorganization involving the creation of the Transportation Security Administration (TSA) in 2001, FAA retained several of its critical aviation security functions in ACS and added responsibilities, such as hazardous materials safety, emergency operations, and intelligence functions.

Today, the FAA mission continues to expand multiple domains in aviation security and safety and must maintain detailed knowledge of the NAS and events that impact civil aviation worldwide to provide command and control communications and situational awareness to the Administrator, Senior FAA leadership, appropriate FAA lines of business and staff offices, National Transportation Safety Board (NTSB), federal officials, interagency security partners, and other aviation entities. ASH, the Office of National Security Programs and Incident Response (AXE), and the Command and Control Communications (C3) Division, are tasked with the mission to provide Information Technology (IT) services and related infrastructure and field equipment needed to support the FAA with emergency operations and Continuity of Operations (COOP) in accordance with Federal Continuity Directive (FCD) 1, FCD 2, and internal FAA orders and directives.

To support its mission, the C3 Program developed an internal set of integrated web-based emergency operation and information-sharing tools called the Emergency Operations Network (EON). Collectively, these tools provide an effective collaborative communications, COOP and adaptive situational awareness platforms that enables the FAA to create a common operational picture and support FAA leadership with data-driven risk-informed decisions.

The PII in EON is used to send notifications of critical NAS events, via email or mobile phone, through the ENS to FAA employees and contractors including members of the public (law enforcement and other members of the aviation community) to ensure the safety and security of the national airspace. The FAA does not use PII for any other purpose.

System Overview:

The EON system is an internal set of integrated web-based emergency operations and information-sharing tools, built on technologies comprised of custom web applications, commercial off-the-shelf (COTS) software, application programming interfaces (APIs), and web services. EON COTS software consists of Environmental Systems Research Institute (Esri)

Geographical Information System (GIS), and Microsoft SharePoint. The GIS component enables the FAA to create maps, compile geographic data about aviation related events, and to analyze and share mapped information with internal FAA stakeholders. The SharePoint component allows the FAA to store, search, track, manage, collaborate, and report on documents and content to support the FAA internally with emergency operations and COOP activities. The APIs and web services enable EON to integrate services with ENS, GIS, SharePoint, and other internal FAA systems to communicate and exchange data.

The C3 Program created the following applications to support its mission and purpose:

EON Daily Report Application (DRA) and Washington Operations Center Operations (WOC Ops) Page – The EON DRA and WOC Ops Page are internal FAA custom web applications developed to assist FAA Operation Centers with (1) the collection of significant and emerging events or security incidents involving the NAS and FAA assets, and (2) the communication of relevant events to FAA stakeholders. DRA supports the Regional Operations Centers (ROC) with collection and reporting of information related to incidents handled by the ROCs and with communication of regional emergencies to regional facilities, other federal agencies, and aviation communities. WOC Ops Page supports the WOC with collection and reporting of information related to incidents handled by the WOC and with communication of regional/national emergencies to federal officials.

EON Esri GIS Technology – EON utilizes Esri GIS technology to support FAA with emergency operations by providing data visualization services. Through this technology, EON offers a mapping portal and dashboard capabilities to support the FAA with collaboration, sharing, tailoring and customization of maps to display FAA assets within maps, including emerging events, trends, and occurrences of incidents within the NAS. The dashboard component enables the FAA to manage, organize, and display metrics into graphs and related charts to assist with analysis and reporting of complex data. Dashboards provide data visualization and situational awareness to FAA Senior Officials about emerging events with potential impacts to FAA assets and the NAS. Other data visualization tool using Esri GIS include EON Home and EON Earth. These tools display predefined maps, with FAA defined map layers, to provide situational awareness about emerging events in the NAS, including data about FAA assets.

EON SharePoint – The EON SharePoint instance is built on Microsoft SharePoint to enable FAA users to store, search, track, manage, collaborate, and report on documents and content within the FAA.

EON APIs and Web Services – The EON APIs and Web Services are internal custom services developed to facilitate the integration of services with ENS, GIS, SharePoint and other internal FAA systems for the communication and/or exchange data to support emergency operations and COOP activities.

EON is not publicly available and is only accessible within the FAA network by FAA employees and/or contractors using their FAA issued Personal Identity Verification (PIV) credentials. EON users primarily are comprised of personnel supporting emergency operations and continuity programs for the Agency including personnel from the Washington Operations Center Complex (WOCC) and ROC.

Operational Use:

FAA Operations Centers play a key role in providing timely notification to the appropriate authorities that there is an emerging air or ground related incident involving the NAS. One of their primary functions is to maintain detailed knowledge of the NAS and other emerging events with potential impacts to state/regional/local and civil aviation worldwide. They provide command and control communications and situational awareness to appropriate FAA offices, NTSB, Federal officials, interagency security partners, and other aviation entities.

There are over 30 different types of aviation incidents, some of great significance which include, but are not limited to, aviation security incident/threat, air carrier accident/incident, pilot deviation, general aviation accident/incident, laser event, medical emergency, unmanned aircraft systems (UAS) (also called a drone) incident. Other events communicated through the operations centers include man-made or natural hazards events with potential impacts to FAA assets and the NAS.

EON assists FAA Operations Centers with the communication of emerging events to the FAA. When an emerging event is reported to an FAA operations center facility, the operations officer on duty follows procedures outlined in DOT/FAA Orders such as JO 8020.16C, 8020.11D, 1910.1K and Agency-specific emergency operating procedures to perform duties as assigned. This includes logging reportable emerging events of significance in EON and communicating the event to relevant FAA stakeholders.

Reported incidents may come from sources internal or external to the FAA via email or phone. Internal sources may consist of FAA personnel from various internal organizations such as the Air Traffic Organization (ATO) or the Office of Aviation Safety (AVS), and/or the Comprehensive Electronic Data Analysis and Reporting system through emails. External sources consist of the public, local emergency organizations, inter/intra agency partners or other aviation entities. Events relating to aviation accidents/incidents typically will contain (1) aircraft type; (2) aircraft registration number[2] "N Number"/call sign[3]; (3) date and time of the accident/incident; (4) position of the aircraft with reference to some defined geographical point or airport; (5)

[2] An aircraft registration, alternatively called a tail number, or N-Number, is a code unique to a single aircraft, required by international convention to be marked on the exterior of every civil aircraft. The registration indicates the aircraft's country of registration, and functions much like an automobile license plate or a ship registration. A privacy concern is that some smaller aircraft call signs may be their N-Number/tail number. In these instances, the N-Number may be linked to an individual via query of another public source.

[3] The call sign and N-Number are not the same. All planes have an N-Number, but not all planes have a call sign

description of the accident/incident, the weather and the extent of damage to the aircraft, so far as is known; and (6) reporting source (organization name and/or air traffic control facility name), where the only PII relates to the call sign or N-Number. This information is essential in providing FAA Operations Center facilities with the minimum amount of information needed to provide timely notification to the appropriate FAA stakeholder. Other logged events do not contain any PII. Only FAA authorized users within the FAA network and with FAA PIV credentials can sign into EON, log the event, and disseminate a notification.

In certain instances, FAA ATO submits security incident reports to FAA Operations Centers via email. The incident report(s) contain information about the pilot/airman involved in the incident, such as name, phone number, certificate number, aircraft registration number/N-Number/call sign, flight number, and a description of the incident. They may also contain contact information about the air traffic control operator on duty such as name, work email and phone number, and contact information from other federal officials and/or interagency security organizations involved in the investigation of the incident such as organization name, work email and phone number.

Emerging aviation accidents/security incidents require immediate and reliable notification, per FAA Order JO 1030.3, to support emergency response and crisis communications activities, and maintain business continuity. To support quick and reliable delivery of notifications, the FAA integrated the EON system with the FAA ENS to leverage the ENS delivery notification services and predefined distribution lists. Through this integration EON (FAA System) and ENS (FAA System) can exchange data, allowing the EON system to promptly disseminate notifications about emerging aviation security events to FAA stakeholders. Disseminated notifications include the following content: date/time of the incident, reporting organization/facility, the N-Number and/or call sign, the aircraft type, and a description and location of the aviation incident/accident. This information is essential in providing FAA stakeholders with the minimum amount of information to perform their organizational duties in maintaining public and aviation safety and security. No other PII is disseminated outside the FAA, and no other notifications contain PII.

Incidents logged into EON are tagged with the geographical location in maps using Esri GIS technology, a process by which GIS adds geographic identification metadata such as co-ordinates (latitude and longitude). EON is able to load other data such as weather and/or natural hazard metadata from sources such as the National Oceanic and Atmospheric Administration or U.S. Geological Survey to enhance the data visualization. This enables the FAA to visualize trending events, their occurrences and potential weather or natural hazards impacts to the FAA within a U.S. geographic location. The resulting map tagged with the geographical location enhances the FAA ability to create a common operational picture of aviation events occurring in the NAS and assist FAA leadership with data-driven risk-informed decisions regarding public and aviation safety and security including national security.

FAA operations officers (FAA employees) can access the EON Mapping Portal to access GIS maps and zoom into a specific US geographic location to view details about logged event(s).

Events related to aviation security only contain and display the following metadata: date/time of the incident, reporting organization/facility, the N-Number, the aircraft type, and a description and location of the aviation incident/accident. Other events displayed in EON maps may consist of weather or natural hazard events such as floods, fires, or earthquake with potential impacts to FAA assets and/or the NAS. These types of events do not contain, nor display, any PII.

EON Dashboards, another function of the EON Mapping Portal, assist FAA personnel in managing, organizing, and displaying important information about certain events with potential impacts to FAA facilities, personnel and/or the NAS to internal FAA stakeholders. EON dashboards do not collect any specific types of information, but rather provide the mechanism to aggregate data from sources within EON and/or FAA systems to display metrics, trends and statistics about certain events being tracked by the FAA into a collection of related charts. Using EON Dashboards, FAA can visually communicate data-driven metrics to help internal FAA stakeholders understand complex issues and report on key information to FAA decision makers and support them with risk-based decisions regarding public and aviation safety and security and/or national security.

EON users can search details of the logged event using the aircraft call sign or N-Number or other fields such as date/time, aircraft type, and location. Alternatively, EON users may use the EON Mapping Portal to access event information contained within dashboards and displayed them within maps.

EON SharePoint allows FAA operations officers, FAA emergency planners, FAA COOP cadre personnel, and the FAA C3 Program staff to internally store, search, track, manage, collaborate and report on documents and content to effectively support the FAA with emergency operations and COOP activities. Among documents and content stored in SharePoint, FAA personnel supporting emergency and continuity of government programs store and manage rosters of key personnel with mission essential responsibilities.

EON contains PII on FAA/DOT employees and contractors such as the name, position/title/region, work location/address, work/personal phone numbers, non-government email address and phone number (provided at the employee's discretion). Other PII, on other employees of federal, state, and local agencies, which is publicly available, includes name, position/title/region, work location/address and phone number.

FAA ATO submits certain security incident reports to FAA Operations Centers via email in the form of file attachments. These reports contain information such as the name of the pilot/airman involved in the incident, as well as his or her phone number, certificate number, aircraft registration number/N-Number/call sign, flight number, and a description of the incident. Additionally, these attachments may include information about the air traffic control operator on duty which includes, name, work email and phone number. Finally, the attachments may include the organization name, work email and phone number of other federal officials and/or interagency security organizations involved in the incident investigation.

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[4]*, 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*[5]*.*

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.

EON is a privacy-sensitive system because it maintains collects, uses, disseminates, and retains PII from pilots, law enforcement, and others in the aviation communities, as well as FAA/DOT employees and contractors, for command and control communications and situational awareness with the purpose of providing IT services and related infrastructure, and field equipment needed to support the FAA. Policies, procedures and practices for information storage, data use, access, notification, retention, and disposal are described herein this PIA.

All PII maintained in EON comes from other sources and is not collected from the individual by EON. All consent mechanisms, including Privacy Act Statements (PAS), are handled by the systems that collect the information.

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 emergency contact records about DOT personnel (including employees, detailees and contractors personnel) that administer emergency-related programs (such as emergency response and continuity of operations). The records contain personal contact information and may include the following PII about DOT personnel: Personal cell phone number and email address.

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

[5] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

DOT/ALL 16, Mailing Management System, 71 FR 35319 (June 19, 2006) covers public contact information for members of the public and Department of Transportation and other government agency employees who have requested to receive notifications from FAA about NAS incidents affecting aviation safety and security and/or are assigned a job role to support FAA emergency related programs.

DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002) covers login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the EON program and/or manage the system.

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

Under the provisions of the Privacy Act, an individual wishing to know if their record exists in EON may submit a request in writing to the below address. Individuals contesting information about their PII contained in EON should make their requests in writing, detailing the reasons why the records should be corrected. Personnel within ASH and AXE, who are responsible for maintaining emergency-related programs, review records periodically and contact personnel members to review their personal information stored in EON. Individuals (requesters) may contact emergency-related programs and/or offices identified above to have their records updated. The requester must provide suitable identification to validate his or her identity before a record can be changed.

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 record(s)
- If contesting, provide detail reasons of why the record(s) should be corrected

Individuals wanting to contest information about themselves that is contained in EON should make their requests in writing, detailing the reasons for 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.

The PII in EON is used to send notifications of critical NAS events, via email or mobile phone, through the ENS to FAA employees and contractors including members of the public (law enforcement and other members of the aviation community) to ensure the safety and security of the national airspace. The FAA does not use the PII for any other purpose.

Congress authorized the FAA Administrator to develop systems and/or tools to support emergency and continuity of operations for the purpose of continuity of government and aviation security and safety. EON addresses the unique demands of the FAA's workforce and operates under the following authorities:

- Public Law 93-366[6]
- Public Law 112-95 Section 333[7]
- 49 USC 40101[8]
- 49 USC 40103[9]
- National Communications System Directive (NCSD) 3-10[10], Minimum Requirements for Continuity Communications Capabilities
- National Security Presidential Directive (NSPD) 51[11] and Homeland Security Presidential Directive (HSPD) 20[12]: National Continuity Policy
- FCD 1[13] and FCD 2[14]

[6] Public Law 93-366 - https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg409.pdf
[7] Public Law 112-95 Section 333 - https://www.govinfo.gov/content/pkg/PLAW-112publ95/pdf/PLAW-112publ95.pdf
[8] 49 USC 40101 - https://www.govinfo.gov/content/pkg/USCODE-2015-title49/pdf/USCODE-2015-title49-subtitleVII-partA-subparti-chap401-sec40101.pdf
[9] 49 USC 40103 - https://www.govinfo.gov/content/pkg/USCODE-2011-title49/pdf/USCODE-2011-title49-subtitleVII-partA-subparti-chap401-sec40103.pdf
[10] NCSD 3-10 - https://www.hsdl.org/?abstract&did=13884
[11] NSPD 51 - https://www.hsdl.org/?abstract&did=776382
[12] HSPD 20 - https://www.hsdl.org/?abstract&did=473297
[13] FCD 1 - https://www.hsdl.org/?abstract&did=729961
[14] FCD 2 - https://www.hsdl.org/?abstract&did=809993

EON collects PII for the following purposes:

- EON System access and program management
  - From FAA employees and contractors: FAA email or username, work and personal phone number, work location/address
- Disseminate Emergency Notifications
  - From FAA employees and contractors: FAA employees and contractors emergency points of contacts, position, work location/address, work and personal phone number, title/region/position, non-government email, address, and phone number.
  - From members of the public including other Federal/state/local agencies, law enforcement, and others in the aviation community: name, position, work location/address, work phone number and the pilot/airman name, address, phone number, Certificate Number, N-Number, flight number, call sign, and incident type involved in the reported incident.

File attachments from reported NAS incidents contain PII from members of the aviation community, such as a law enforcement point-of contact on duty during the reported incident, and may include the name, work email/phone number. Also, data from the air traffic facility point-of-contact on duty during the reported incident, which is publicly available, may include the name, work email, and phone number.

EON uses this information in accordance with the purposes for which it is collected under DOT/ALL 22, *Emergency Contact Records (ECR)- Not Covered by Notices of Other Agencies*, 75 FR 68852 (November 9, 2010); and DOT/ALL 16, *Mailing Management System*, 71 FR 35319 (June 19, 2006), which provides the purpose of collection for contact records that are used by FAA/DOT 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.
- 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 provide notification of critical NAS security incidents including other events affecting aviation safety and security.

Access and authentication records within EON are handled in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002).

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.

FAA personnel collects the minimum amount of information from individuals to support FAA's emergency related programs. Related records are maintained in accordance with National Archives and Record Administration (NARA) approved General Retention Schedule (GRS) 5.3, Item 020, Employee Emergency Contact Information DAA-GRS-2016-0004. These contact records are destroyed when they are either superseded or obsolete, or upon separation or transfer of employee.

Employee directories within EON that contain information about where employees are located in facilities and work phone numbers will be maintained in accordance with GRS 5.5, Item 20 DAA-GRS-0012-0002. The records are destroyed when they are one year old or when they are superseded or obsolete, whichever is applicable, but longer retention is authorized if the records are required for business use.

Information in EON including login credentials, audit trails, and security monitoring are retained until business use ceases in accordance with NARA GRS 3.2, September 2016, *Information Systems Security Records*, System Access Records.

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.

The PII in EON is used to send notifications of critical NAS events via email or mobile phone through the ENS to FAA employees and contractors including members of the public (law enforcement and other members of the aviation community) to ensure the safety and security of the national airspace. The FAA does not use the PII for any other purpose.

The FAA/DOT limits the scope of PII collected in EON to support the purpose specified in SORN *DOT/ALL 22, Emergency Contact Records (ECR)- Not Covered by Notices of Other Agencies*, 75 FR 68852 (November 9, 2010) and DOT/ALL 16, *Mailing Management System -* 71 FR 35319 (June 19, 2006). FAA/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, 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. Access and authentication records within EON are handled in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002).

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).

EON is an internal system and is not public facing. Data entry, quality and integrity are handled by FAA personnel. FAA employees, contractors, interagency security partners, and members of the public, such as members of the aviation community who wish to receive notifications about safety/security aviation incidents, are responsible for providing accurate organization contact information to the FAA Operations Centers. The FAA Operations Centers follow standardized process and procedures when collecting aviation safety incident data reported by FAA/ATO or external sources such as Federal/state/local agencies and/or law enforcement agencies. For NAS-related incidents/accidents, the information entered in EON is only as accurate as the information provided by the reporting source. EON has following procedures and processes in place to ensure that once the program receives the information, it is as accurate, relevant, timely, and complete as possible:

- Access control mechanisms to ensure only authorized personnel can create, update, delete data from the system (e.g., security groups in Active Directory or role-based access)
- Encryption to protect data stored in the database from unauthorized access (e.g., FIPS-142/143 Cryptographic Algorithms)
- Hashing algorithms to prevent data from changes (e.g., FIPS-142/143 Cryptographic Algorithms)
- Identity and authentication level of assurance (e.g., Identity Credential & Access Management (ICAM) or as FAA calls it MyAccess)
- Public Key Infrastructure (PKI) (e.g., Web or SSL certificates to ensure data in transit is encrypted and protected)

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 Publication 200, dated March 2006, and the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated April 2013.

These safeguards include an annual independent risk assessment of the EON 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 EON. All data in-transit is encrypted and access to electronic records is controlled by PIV and 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 EON an on-going authorization to operate.

Other safeguards incorporate standards and practices required for federal information systems under 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.

Lastly, access to the EON system from the public internet is not permitted and the system is only accessible to authorized FAA personnel from within the FAA Intranet.

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 1370.121, as amended, 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, as amended. The FAA will conduct periodic privacy compliance reviews of EON as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Kevin Van Haren
System Owner
Branch Manager, Emergency Communications (AXE-410)

Prepared by: Barbara Stance

Approval and Signature

Karyn Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer