U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

iConect Litigation Tracking System (iConect)

Responsible Official

Carl Edwards
carl.edwards@faa.gov
(202) 267-3936

Reviewing Official

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

Executive Summary

The Office of Chief Counsel (AGC) within the Federal Aviation Administration (FAA) uses iConect Litigation Tracking ("iConect") system, a web-based (Intranet) mission support commercial off-the-shelf (COTS) litigation management software tool and in-house electronic document discovery repository system by iConect Development, LLC, for multi-party litigation support and collaboration for personnel class action cases. The system manages all documents necessary for processing a case and any documents received electronically. It includes a document assembly system to create documents, a document management system to manage and store documents, and a case management system to record activities in cases and track case files. The system supports the agency's mission by providing a single collection point for employment and labor law litigation documents and information.

The FAA is publishing this Privacy Impact Assessment (PIA) for the iConect Litigation Tracking system 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 citizens or Legal Permanent Residents (LPR), members of the DOT Contract workforce, and members of the DOT Federal workforce.

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:

[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).

- *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

The Office of Chief Counsel (AGC) uses iConect as a litigation tracking system to manage all documents necessary for the processing of administrative and court litigation matters, or FAA policy relating to the employment of FAA personnel. iConect is deployed at the Office of Information and Technology Services-Enterprise Data Center (AIT-EDC) at the William J. Hughes Technical Center (WJHTC) in Atlantic City, NJ.

iConect is an internal, web-based electronic document discovery system designed to create, manage, and store documents, and manage cases to record activities in cases and track case files. iConect contains documents FAA attorneys need during discovery in litigation, which includes employment applications. The Office of Chief Counsel Employment and Labor Law Division (AGC-100) uses the information and data maintained in iConect to represent the FAA in administrative and court litigation matters, to provide advice on FAA policy relating to the employment of FAA personnel, and in all labor and employment-related cases originating at the FAA. Employment and Labor Law Division attorneys represent the FAA before the Equal Employment Opportunity Commission (EEOC), the Merit Systems Protection Board (MSPB), in matters before the Office of Special Counsel (OSC), and in selected Federal Labor Relations Authority (FLRA) proceedings and negotiated grievance procedure arbitrations.

The system maintains documents produced in discovery, which include, in part, select files (with applications that include names, addresses, phone numbers, etc.). Employment and Labor Law Division Attorneys primarily use the documents and information when preparing to represent the FAA in administrative and court litigation, grievance arbitrations, and cases related to challenged employment actions. Images of legal documentation are scanned and stored in the systems as records, which authorized personnel can retrieve through the application interface. The system deals only with information about current and former Department of Transportation (DOT) Federal employees and applicants for employment involved in employment class action suits. iConect contains files and data derived from other data sources and facilitates searches and processing of those records for discovery and other litigation-related purposes.

iConect only contains copies of information located in other systems and serves to facilitate searches and processing those records for discovery and other litigation-related purposes. As a result, documents and information maintained within iConect are not the official recordkeeping copies of the records.

iConect contains the following PII from members of the public and the FAA employee and contractor workforce who are the subject of cases involving hiring or promotion actions:

- Full name (applicants, which includes contractors and FAA employees)
- Mailing address
- Social Security Number (SSN)
- Telephone number (work or personal)
- Employee ID number
- Date of Birth (DOB)
- Education and work history
- Employee Position Data (title/grade/agency/branch/unit)
- Full name of selectee
- Full name of reference(s)
- Exhibits (photos, memos, and correspondence)

iConect is only used by AGC-100 and their support staff, who are FAA employees and FAA contractors. Only these approved users are granted access to iConect. Users access iConect at Uniform Resource Locator (URL) https://agcic.faa.gov via multi-factor authentication. iConect users connect to the website via their Personal Identity Verification (PIV) card through MyAccess, which manages identity verification and authentication for non-DOT affiliated individuals requiring access to DOT and FAA applications on the FAA network. Upon visiting the website, users are prompted to enter their iConect user account information into the iConect database. Periodically, the iConect system owner conducts access reviews for role changes or when an FAA employee or contractor has left the agency and emails the system administrator to remove access from those iConect users. Members of the public do not have access to iConect.

The iConect system contains information pertaining to current DOT employees, former DOT employees, and applicants for DOT employment. iConect contains only information on individuals who are involved in employment class action suits in administrative and court litigation, grievance arbitrations, or other challenged employment actions. iConect contains copies of legal documents, files including pleadings, discovery materials, motions, briefs, exhibits, interrogation, interoffice communications, memoranda, orders, and other correspondence related to a litigation matter, as well as data derived from other data sources. iConect does not share any data with any other FAA systems other than MyAccess. System administrator scan and upload copies of legal documents into iConect. Authorized users cannot modify uploaded documents. The Office of the Chief Counsel (AGC-100) receives these legal documents through the legal discovery process from other offices depending on the subject matter of the litigation. AGC-100 receives hard-copy documents

that are uploaded or compact disks (CDs) that contain the documents. All PII ingested by iConect originate from these uploaded CDs or documents from courts and litigation sources. All hard-copy files and CDs are locked in a fireproof safe within the Chief Counsel's Office as a source of backup to the files. The CDs and hard copy documents are maintained and disposed of in accordance with the appropriate National Archives Records Administration (NARA) disposition schedule depending on the contents of the document.

Authorized users retrieve documents in iConect to assist in their job functions at the following stages of the case process:

Central Personnel Management

Central personnel management maintains and provides up-to-date, and accurate personnel data from hiring to firing an employee. The cover page from applications submitted by current and former FAA employees and contractors includes personally identifiable information (PII) such as full name, position, title, Social Security number (SSN), date of birth (DOB), and the full name of any referrals. AGC attorneys collect and upload this information into iConect to manage and record activities in cases.

Litigation and Judicial Activities

AGC attorneys and support staff manually upload all documents related to the legal proceeding, such as discovery files, witness statements, interviews, and pleadings from litigants and defendants, which are filed with the court or administrative body. AGC staff review these documents and, if necessary, redact information, date-stamp them, and/or mark them as privileged. These documents may contain PII, such as the full names of applicants, which could include those of FAA employees and contractors, their official positions and titles, DOB, SSN, pleadings, and the full names of referrals.

Legal Prosecution and Litigation

iConect maintains all documents collected and uploaded to represent the agency in matters before the EEOC. The documents collected and uploaded include responses to discovery as well as additional documentation related to the agency's defense in the case. The PII contained in these uploaded documents may include, but is not limited to, the following: full names, positions, and titles, SSN, DOB, full names of referrals, motions, exhibits, briefs, and interoffice communications with email addresses, applicant resumes and work histories, education transcripts, and full names and contact information of opposing counsel if included in the correspondence.

Legal Resolution

AGC staff uploads a copy of the settlement agreement, if applicable, for the matter, along with any other documents related to the resolution discussions. The PII contained in these documents are uploaded and may include, but are not limited to, the following: the applicant's full name (including FAA employees and contractors), the authorized official's full name and signature

approving the settlement agreement, SSN, DOB, position and title, the full name and signature of the authorized litigant, and the full name and signature of the litigant's authorized agency.

iConect is a stand-alone system and does not share any information with any other system, nor does it receive any information from any other system. iConect sends a user's email address to MyAccess for authentication purposes into the system. iConect generates ad-hoc aggregate reports for any data filed within the system.

iConect generates and maintains audit logs that monitor account management changes, login activity, and system events, which the system owner reviews to ensure proper use of the system. The audit logs contain employee user IDs, time, date, and any actions taken, such as editing or adding data, within the system by a user.

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[2], 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[3].

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.

iConect Litigation Tracking system is a privacy-sensitive system because it collects, uses, disseminates, and retains PII from current and former FAA employees, current and former FAA contractors, and members of the public who have applied for FAA employment. Policies, procedures, and practices for information storage, data use, access, notification, retention and disposal are described herein this PIA. The FAA employs multiple techniques to ensure individuals are aware of iConect and how the FAA collects and maintains PII in support of iConect.

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

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

DOT/FAA 821, *Litigation Information Management Systems,* 65 FR 19522 (April 11, 2000),which provides notice of the privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of personnel and general litigation records of litigants, claimants, decedents, the plaintiff's attorney, FAA attorney, and Department of Justice attorney.

DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002), which covers verification and authorization records along with user access records to the DOT's office automation network. It also includes records denials of access for purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors involved in the iConect program and/or manage the system. This usage aligns with the description in the "purpose" section of DOT/ALL 13.

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

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, 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.

iConect receives and maintains records that may contain names, SSNs, employee identification numbers, home address, or phone numbers originated by the government that identify a particular individual. iConect does not collect PII directly from individuals. iConect stores and maintains uploaded documents that may contain PII.

Under the provisions of the Privacy Act, individuals may request searches of the iConect system to determine if any records may pertain to them and if such records are accurate. Individuals wishing to know if their records appear in this system may inquire in person, or in writing to:

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

Individuals wanting to contest information about themselves that is contained in iConect should make their request in writing, detailing the reasons why their records should be corrected and addressing their letter to the following address:

Federal Aviation Administration

Privacy Office

800 Independence Avenue, SW

Washington, DC 20591

If you have comments, 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 the business need for an internal, web-based electronic document discovery system. This system creates, manages, and stores documents, while also tracking case files and recording activities to manage cases. SSNs are collected from members of the public applying for agency positions by the FAA's Office of Human Resources (AHR). iConect addresses the unique demands of the FAA's workforce and operates under the authority under Executive Order 9397, as amended by Executive Order 13478, United States Code (U.S.C.) 1302, 3109, 3301, 3304, 3305, 3307, 3309, 3313, 3317-3319, 3326, 4103, 5533 and 7201; and 29 Code of Federal Regulations (CFR) 720.301 which is the policy of the United States that Federal agencies, that any activity that involves personal identifiers do so in a manner consistent with protection of such identifiers against unlawful use.

The underlying authority for maintenance of the records that have been uploaded into iConect for litigation purposes as follows: Title VII of the Civil Rights Act of 1964 (Pub L 88-352) (Title VII), as amended, appears in volume 42 of the United Stated Code, beginning at section 2000e; enforces the constitutional right to prevent discrimination in federally assisted programs to establish a Commission on Equal opportunity, and for other purposes; Age Discrimination in Employment Act of 1967 (Pub L. 90-202) (ADEA), as amended volume 29 of the United States Code, beginning at section 621; prohibits age discrimination in employment; Equal Pay Act of 1963 (Pub L. 88-38) (EPA), as amended, appears in volume 29 of the United States Code, at section 206(d); prohibits discrimination on account of sex in the

payment of wages by employers engaged in commerce or in the production of goods for commerce; Fair Labor Standards Act of 1938, which provides for the establishment of fair labor standards in employment in and affecting interstate commerce and for other purposes and DOT/FAA 821 - Litigation Information Management Systems, 65 FR 19522 (April 11, 2000) which provides a routine use of records in the system to disclose them to the Department of Justice or other Federal agencies conducting litigation.

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 iConect uses data minimization techniques in addition to appropriate retention policies to reduce the privacy risks associated with the project. iConect collects the minimal amount of data that is relevant and necessary to create, manage, and store documents, as well as to manage cases, record activities, and track case files.

iConect records are maintained in accordance with NARA) The General Technology Management records are maintained in accordance with NARA General Records Schedule (GRS) 3.1, item 20, General Technology Management Records, approved November 2019. Information Technology Operations and Maintenance records pertain to the activities associated with the operations and maintenance of the basic systems and services used to provide the agency and its staff with access to computers and data telecommunications. Includes activities associated with IT equipment, IT systems, storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure.

These records are temporary and are destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded. Information may be retained for longer timeframes if required for business purposes.

System access records maintained under GRS 3.2. item 30, Information Systems Security Records These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. These records include user profiles, log-in files, password files, audit trail files and extracts, system usage files, cost-back files used to assess charges for system use. These files are temporary and are destroyed when business use ceases.

The Common Office records are records that are non-official record keeping copies of electronic records. These records are maintained in email systems, computer hard drives or networks, webservers, or other locations after agencies copy the records to record-keeping system or otherwise preserve the record-keeping version. Records include documents (letters, memos, reports, handbooks, directives, manuals, briefings, or presentations created on office applications, including those in Portable Document Format (PDF) or its equivalent, senders‘ and recipients’ versions of electronic mail messages that meet the definition of Federal records, and any related attachments,

electronic spreadsheets, digital still pictures or posters, digital video or audio files, digital maps or architectural drawings, and copies of the above electronic records maintained on websites or webservers, but excluding web pages themselves. These records are maintained in accordance with GRS 5.1, Item 20, Common Office Records, are temporary and are destroyed immediately after copying to the official recordkeeping system. The temporary records may be retained for longer timeframes if required for business purposes.

All hard-copy files and CDs are locked in a fireproof safe within the Chief Counsel's Office as a source of backup to the files. The CDs and hard copy documents are maintained and disposed of in accordance with the appropriate National Archives Records Administration (NARA) disposition schedule.

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.

iConect receives and maintains records that may contain name, SSNs, or other numbers originated by the government that identify a particular individual, such as employee identification number, home address, phone numbers, and education records. These records are maintained to assist agency counsel in preparing to represent the FAA in administrative and court litigation suits, proceedings and negotiated grievance procedure arbitrations, and cases related to challenged employment actions. iConect includes documents incidental to a lawsuit, including pleadings, discovery materials, motions, briefs, exhibits, interrogatories, interoffice communications, memoranda, orders, and correspondence with opposing counsel, and joint counsel, some of which contains SSNs.

Additionally, iConect does not share information or any data exchanges with external systems. There is no external sharing, and no external sharing is authorized.

The PII in the iConect system is not routinely used for any other purposes

The FAA/DOT limits the scope of PII collected in iConect to support case management/record management as specified in SORN DOT/FAA 821, *Litigation Information Management Systems,* 65 FR 19522 (April 11, 2000). Access and authentication records within iConect are handled in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002).

The Department has also published 15 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."

DOT/FAA 821 Routine Uses

- For Law Enforcement Purposes--To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where OPM becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.
- For Certain Disclosures to Other Federal Agencies--To disclose information to a Federal agency, in response to its request in connection with the hiring or retention of an employee, the issuance of a security clearance, the conducting of a suitability or security investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter
- For Congressional Inquiry--To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.
- For Judicial/Administrative Proceedings--To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding. In those cases where the Government is not a party to the proceeding, records may be disclosed if a subpoena has been signed by a judge.
- For National Archives and Records Administration--To disclose information to the National Archives and Records Administration for use in records management inspections.
- Within OPM for Statistical/Analytical Studies--By OPM in the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies. While published studies do not contain individual identifiers, in some instances the selection of elements of data included in the study may be structured in such a way as to make the data individually identifiable by inference.
- For Litigation--To disclose information to the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which OPM is authorized to appear, when: (1) OPM, or any component thereof; or (2) Any employee of OPM in his or her official capacity; or (3) Any employee of OPM in his or her individual capacity where the Department of Justice or OPM has agreed to represent the employee; or (4) The United States, when OPM determines that litigation is likely to affect OPM or any of its components; is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or OPM is deemed by OPM to be relevant and necessary to the litigation provided, however, that the disclosure is compatible with the purpose for which records were collected.
- For the Merit Systems Protection Board--To disclose information to officials of the Merit Systems Protection Board or the Office of the Special Counsel, when requested in

connection with appeals, special studies of the civil service and other merit systems, review of OPM rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions, e.g., as promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

- For the Equal Employment Opportunity Commission--To disclose information to the Equal Employment Opportunity Commission when requested in connection with investigations into alleged or possible discrimination practices in the Federal sector, compliance by Federal agencies with the Uniform Guidelines on Employee Selection Procedures or other functions vested in the Commission and to otherwise ensure compliance with the provisions of 5 U.S.C. 7201.
- For the Federal Labor Relations Authority--To disclose information to the Federal Labor Relations Authority or its General Counsel when requested in connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.
- For Non-Federal Personnel--To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government

DOT/All 13 Routine Uses are as follows:

- To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.
- To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.
- To contractors, grantees, experts, consultants, detailers, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records.
- To other government agencies where required by law.

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).

iConect contains copies of files and data derived from other data sources. iConect does not share any data interconnections with systems other than MyAccess, for their data source. AGC-100 personnel must have an iConect account to access the iConect database. Periodic account reviews track job changes and identify individuals who have left the company.

Only AGC-100 personnel scan and upload copies of legal documents into iConect. Authorized users cannot modify uploaded documents. iConect generates and maintains audit logs that monitor changes in account management, login activities, and system events. The system owner reviews these logs to ensure proper usage. The audit log records employee user IDs, the date and time of each action, and any actions taken by users, such as editing or adding data within the system. AGC-100 receives these legal documents through the legal discovery process from other offices depending on the subject matter of the litigation. Also, individuals can request searches of the iConect system to verify the accuracy of records. They may submit their inquiries in person, or in writing. If individuals contest information about themselves contained in iConect, they make their request in writing, detailing the reasons for requesting corrections to their records. AGC-100 receives hard-copy documents that are uploaded or compact disks (CDs) that contain the documents. All PII ingested by iConect originate from these uploaded CDs or documents.

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).

The iConect system has met all requirements and has been certified with an Authority to Operate (ATO) by DOT/FAA. iConect was granted its ATO on September 23, 2024, after undergoing the National Institute of Standards and Technology (NIST) security assessment and authorization (SA&A). FAA Security Personnel audit iConect to ensure FISM compliance through an annual assessment according to NIST standards and guidance.

The FAA implements security and privacy controls that fully incorporate administrative, technical, and physical measures to protect users' PII against loss, unauthorized access and disclosure. All data in-transit is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN), and access is limited according to job function. Additionally, FAA conducts an 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 iConect 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.

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.

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.

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 iConect 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 iConect as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Name: Carl Edwards
Email: carl.edwards@faa.gov
Phone Number: (202) 267-3936

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2026.01.09 13:59:46 -05'00'