U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Air Traffic Organization (ATO)

Quota Management and Resource Tool (QMART)

Responsible Official

Sherri Cottle
Email: sherri.cottle@faa.gov
Phone Number: 405-954-7102

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) Quota Management and Resource Tool (QMART) is operated and maintained by the FAA Office of Safety and Technical Training, Technical Training Performance Analysis Team, AJI-2210. QMART is used by FAA employees to monitor and plan enrollments for each fiscal year's FAA Academy training schedule for newly hired air traffic controllers and certified professional controllers. QMART is a web-based application accessible only to users inside the FAA Intranet.

The FAA is conducting this Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 because QMART uses the Personally Identifiable Information (PII) of members of the public who have accepted an offer letter of employment from the FAA to begin training as an air traffic controller. This PIA also addresses the privacy risks for FAA employees who access the system in their official capacity.

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;*

---

[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).

- *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 Federal Aviation Act of 1958 gives the FAA the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. QMART is a web-based application designed to support FAA management in providing the Air Traffic Controller (ATC) workforce the necessary technical and specialized operational training to support the FAA's mission and goals of safety, security, and system efficiency. These standards are required by the Congressional Restrictions on Training first enacted in Section 337 of Public Law 104-50, Department of Transportation Appropriations Act, 1996, and subsequent appropriations.

QMART is an FAA management tool that provides the Office of Human Resource Management (AHR), AJI and the FAA Academy the ability to analyze annual training requirements and develop annual FAA Academy class schedules for the ATC workforce, including ATC candidates or pre-hires.

Pre-hire ATC student enrollments are managed in QMART, and pre-hire class rosters are generated from QMART. Pre-hire students cannot be enrolled in the eLearning Management System (eLMS), the FAA's primary training management system, until the Federal Personnel and Payroll System (FPPS) feeds the new employee information into eLMS to create an employee profile after hire, so the pre-hire student names are entered into QMART to be used by management (AHR, AJI, FAA Academy) for planning and scheduling purposes.

QMART produces training reports and summaries to help manage ATC training. Most reports are of a statistical nature and do not contain PII. Some reports do contain limited PII data, such as class rosters with students' names and their facilities. These reports help instructors know if there are enough students enrolled in a class or whether it should be rescheduled or cancelled. QMART also provides information to the FAA regarding unused training slots, such as in cases where the student did not attend a class or did not complete a class due to an emergency, such as an illness.

Note: the eLMS ID, which is the same as the FAA Employee ID, is not included on the reports; it is only used by the service center training coordinators to verify the correct eLMS

entry if there are multiple students with the same first and last name. Users of QMART search by:

- Employee Name
- Facility ID
- Service area or region
- Course number
- Class number

Typical QMART Transactions for Pre-Hire ATC Students

Pre-hire ATC candidates do not have access to QMART.

Once a pre-hire or ATC candidate signs a final offer letter (FOL) to work for the FAA, AHR schedules them for their Basic and Initial Qualification training. Their start date or enter-on-duty (EOD) date will be their first day of virtual FAA air traffic controller training (ATC Basics). On a weekly basis, AHR compiles a spreadsheet of pre-hires that have been scheduled for ATC training and emails it to the QMART System Administrator (QSA).

One to three weeks before the beginning of the ATC Basics class, the QSA copies the pre-hire ATC information from the spreadsheet into the QMART class record using a copy feature of the QMART application. The QSA can also manually enter the pre-hire information into the QMART class record.

The class training records in QMART for all pre-hires, including those who either decline or resign, are kept in QMART for three years.

The PII for pre-hire ATC students maintained in QMART is name, personal email address, date the new hire plans to onboard (proposed EOD), hiring source (military or civilian), student type (pre-hire or FAA employee), the course they have been assigned, and completion status. The QMART system administrator can add a comment on a record that the pre-hire has declined and date the pre-hire declined.

QMART Users

All QMART users (either FAA employees or contractors) sign into QMART using their Personal Identity Verification (PIV) card. The QMART application authenticates the users via MyAccess and determines the scope and level of access to information within QMART.

Only AHR, QSA, and FAA Academy users have access to pre-hire PII information in QMART.

QMART produces training reports and summaries to help manage ATC training. Most reports are of a statistical nature and do not contain PII. Some reports do contain limited PII

data, such as class rosters with students' names and their facilities. These reports help instructors know if there are enough students enrolled in a class or whether it should be rescheduled or cancelled.

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.

The FAA employs various strategies to ensure that the FAA pre-hires are informed of the purpose for which the FAA collects, uses, disseminates, and retains their PII. Individuals voluntarily apply for FAA positions and provide their own PII as required by the FAA's application process.

Enrollment into air traffic controller training classes is one of the purposes for which the FAA collects PII on pre-hires. QMART is not interconnected with [AVIATOR](#)[4], so an AVIATOR Human Resource Specialist (in Aviation Careers Branch, AHF-S310) generates an Excel spreadsheet of upcoming pre-hires and emails it to the QSA each week.

In QMART, the only users who create an account are the QSA or facility training specialists. They use forms located on the QMART website to create a user account and a

---

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf
[4] AVIATOR is a web-based application used by current FAA employees to develop and post FAA job announcements through a system interface with the Office of Personnel Management (OPM) USAJOBS.gov web-based system, and by members of the public to apply for FAA job openings.

user training assignment. There is a Privacy Act Statement located on these forms apprising users of how the FAA maintains and discloses information.

The FAA retrieves records by an individual's name and other personal identifiers and protects Privacy Act records in accordance with the Department's published system of records notice (SORN):

SORN DOT/ALL 27, _Training Programs_ – 83 FR 60960 – (November 27, 2018). QMART maintains all pre-hire and student class information for three years. eLMS is the official system of record for FAA employee training records – not QMART. QMART is not interconnected with eLMS. DOT/ALL 13, _Internet/Intranet Activity and Access Records_ - 67 FR 30757 (May 7, 2002) covers system access records maintained in QMART.

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.

Individuals who wish to voluntarily apply for an FAA air traffic controller position must create and complete a profile on OPM's USAJOBS, which shares PII with FAA's AVIATOR system. No PII from USAJOBS or AVIATOR is transferred to QMART.

Job seekers voluntarily create profiles in USAJOBS for the purpose of applying for federal jobs. If a job seeker chooses to apply for FAA job, such as air traffic controller, USAJOBS shares specified candidate PII with AVIATOR. Once HR has made a hiring decision and issues an offer of employment, and the individual has signed an offer letter, AHR assigns the individual to the initial air traffic controller classes and includes them on a spreadsheet that is sent to the QMART system administrator (PII is name email, EOD, and class assignments). One to three weeks before the air traffic class begins, the QMART system administrator enters the pre-hire information into QMART either manually or by copying it from the spreadsheet.

Pre-hires do not have access to QMART, but the QSA and the QMART FAA Academy users have edit capability, and they can update pre-hires' information in QMART as needed.

Notification Procedure (for access to records): Under the provisions of the Privacy Act, individuals may request searches to determine if any records in QMART pertain to them. Individuals wishing to know if their records appear may inquire in person or to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue (Ave), 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.

Contesting Record Procedures: Individuals wanting to contest information about themselves that is contained in QMART should provide their request in writing, detailing the reasons for why the records should be corrected and addressing their letter 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 authority for the collection of the information in the QMART system is 5 U.S.C. 301; 23 U.S.C. 504; and 49 U.S.C. 301, 5314, 5315, 20108, 30182, and 40108, which provides the FAA authority to ensure safety in the National Airspace.

QMART is used by FAA AJI to track and monitor the enrollments in air traffic courses. Student information (student names, personal email address, hiring source, student type (pre-hire or FAA employee), start date, course completion status, and course assigned) is manually entered into their assigned classes in QMART. Pre-hire email addresses are used to send welcome letters to the pre-hires prior to the start of training. Welcome letters include class location and start times, instructor contact information, and housing instructions.

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 maintains different types of records in accordance with the following National Archives and Record Administration (NARA) approved General Retention Schedules.

The QMART application collects student names, personal email address, hiring source, student type, start date, course completion status, course assigned for FAA ATC to plan,

schedule, and provide ATC training. This is the minimum amount of information needed to assign a class for new hires who are onboarding to become an Air Traffic Controller.

NARA GRS 5.1, *Common Office Records*, July 2017

- Item 10, Administrative records maintained in any agency office – These records can be destroyed when business ceases. QMART is not the official documents. QMART is a planning and scheduling tool and therefore are considered common office records.

NARA GRS 2.6, *Employee Training Records*, April 2020

- Item 10, Non-mission employee training program records. These records can be destroyed when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.

NARA GRS 3.1, *General Management & Technology Records*, November 1, 2019

- Item 11, System development Records- These records can be destroyed 5 years 2013-0005- after system is 0007 superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

- Item 20, IT Operations & Maintenance Records – These records can be destroyed three years after agreement control measures, procedures, project activity, or transaction is obsolete, completed, terminated, or superseded; but longer retention is authorized if required for business use.

- Item 30, Configuration, and change management records – These records can be destroyed five years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

- Item 51, All documentation for temporary electronic records and documentation not necessary for preservation of permanent records. – These records can be destroyed five years 2013 after the project/activity/ transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.

NARA GRS 3.2, *Information Systems Security Records*, January 2023

- Item 10, Systems, and data security records – Records can be destroyed 1 year(s) after system is superseded by a new iteration or when no longer needed for

agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

- Item 30, System access records – These records can be destroyed when business use ceases.

- Item 40, System backups and tape library records (Incremental backup files) – Records are destroyed when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

- Item 41, System backups and tape library records (Full backup files) – Records are destroyed when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

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.

FAA AHR Administrative Users may share data from AVIATOR with personnel staffing specialists and other authorized employees who have a need to know the information for FAA business purposes. One of these routine uses is sharing AVIATOR data with AJI/Academy/AHR for planning purposes and carrying out the basic ATC training.

The service center training personnel manually enter the enrollments in the eLMS using the QMART data. This task is accomplished by obtaining the student's name, class number and dates from QMART, then finding the corresponding class and student, and entering them into eLMS. The service center personnel may use the eLMS learner ID entered in QMART to ensure the correct FAA employee is enrolled in the class.

QMART receives username and security certificate information from MyAccess for access and authentication purposes.

QMART receives student information from eLMS via manual data entry to document enrollment in training courses. The information QMARTs receives includes student name, class number and class dates. There is no information returned to eLMS from QMART.

The PII that is entered into QMART is used to provide the FAA and its ATC pre-hires with an effective training process. The FAA does not use PII that is stored in QMART for any purposes other than supporting the training process.

Only AHR, QSA or FAA Academy QMART users have access to the pre-hires' PII contained in QMART.

In accordance with the Privacy Act system of records notice, DOT/ALL 27 – Training Programs 83 FR 60960 - November 27, 2018 *Training Programs*, this information is routinely disclosed in the following circumstances: (1) To organizations, including other government entities, sponsoring or providing remuneration for training; (2) To other federal agencies as needed to create class schedules, or determine qualifications for participation in classes as students or instructors; and (3) To educational institutions or training providers as evidence of participation or successful completion, as needed to continue education. There are additional routine uses that exists for this system which is located here. DOT General Routine Uses SORNs | US Department of Transportation.

DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002) covers system access records maintained in QMART.

Data Quality and Integrity

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

The FAA supports the accuracy, relevance, timeliness, and completeness of pre-hire information. The FAA assumes the accuracy of the information in QMART that it receives from AVIATOR (AVIATOR receives the information from OPM's USAJOBS) because the PII is collected voluntarily and directly from the individual pre-hire, and because the individual is required to assert that all information on their FAA job application, including PII, is correct and complete.

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, disclosure or unauthorized access. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in the Federal Information Processing Standards Publication (FIPPS) 200, dated March 2006, and the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated December 2020.

The QMART application meets all requirements and has been certified with an Authority to Operate (ATO) by DOT/FAA. QMART was granted its latest ATO on August 19, 2021, after undergoing a NIST-based security assessment and authorization. QMART is audited by FAA Security Personnel to ensure FISMA compliance through an annual assessment according to NIST standards and guidance.

QMART takes the following steps to safeguard PII:

- Physical security and environmental controls in the data center that houses the QMART servers. Physical access is limited to designated personnel through photo ID badges, building key cards and room-access keypads.
- Data encryption in transit and at rest on QMART database servers.
- PIV identification and authentication required of all QMART users as well as a Privacy Awareness Statement (PAS) displayed on each login.
- QMART user roles and permissions that restrict user access to information to those who have a "need to know."

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.

The FAA's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division is responsible for governance and administration of FAA Order 1730.121A, FAA Information Security and Privacy Program, implements the various privacy requirements of the Privacy Act of 1974, the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, OMB mandates and other applicable DOT and FAA Records Management procedures and guidance. In addition to these practices, the FAA consistently implements policies and procedures, especially as they relate to the access, protection, retention and destruction of PII. Federal and contract employees who work with QMART are given clear guidance in their duties as they relate to the collection, use, processing and security of privacy data. Guidance is provided in the form of FAA 1730.121A, mandatory annual security and privacy awareness training including Rules of Behavior (ROB) Acknowledgement. The FAA Office of the Chief Privacy Officer will conduct periodic privacy compliance assessments of QMART in accordance with the requirements of the OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Sherri Cottle
System Owner
Team Lead, Technical Training Performance Analysis Team (AJI-2210)
Safety & Technical Training (AJI-2)

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer