Office of Inspector General
Audit Report

FAA'S CIVIL AVIATION REGISTRY LACKS INFORMATION NEEDED FOR AVIATION SAFETY AND SECURITY MEASURES

Federal Aviation Administration

Report Number: FI-2013-101
Date Issued: June 27, 2013

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: ACTION: Report: FAA's Civil Aviation Registry Lacks Information Needed for Aviation Safety and Security Measures
Report Number FI-2013-101

Date: June 27, 2013

From: Louis King
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Federal Aviation Administrator

As part of the Federal Aviation Administration's (FAA) safety mission, its Flight Standards Service[1] (AFS) maintains the Civil Aviation Registry to ensure that unqualified aircraft owners and airmen[2] do not receive aircraft registrations or licenses. FAA uses the Registry to process and maintain ownership registrations on 350,000[3] private and commercial aircraft and records on pilots' licenses. The Registry, which contains personally identifiable information (PII), also serves as a source of information for other Government agencies, including those responsible for homeland security and investigations of aviation accidents and other incidents.

We initiated this audit because of congressional concerns over aviation safety and the security of the information that FAA maintains in the Registry. Our objectives were to determine whether (1) aircraft registrations and pilot certifications include the information needed for FAA to ensure aviation safety, (2) security controls keep the Registry secure from unauthorized access, and (3) contingency plans are sufficient to recover the Registry system in the event of an emergency.

To conduct our work, we interviewed officials from FAA's Flight Standards Service and Aviation Safety Office of Quality, Integration, and Executive Services. We reviewed laws governing aircraft registration and pilot certification and examined FAA's policies and procedures on the Registry's operations. We

[1]AFS promotes safe air transportation by setting standards for certification and oversight of pilots; air carriers including major airlines, regional carriers and cargo carriers; flight schools and training centers; and management of the information systems of record for pilots and all civil aircraft.
[2]Individuals certified by FAA's Airman Certification Branch under 14 CFR Aeronautics and Space § 61, 63 and 65.
[3]The number of U.S. civil aircraft registered as of August 2012.

also assessed FAA's compliance with Department of Transportation (DOT) policy on maintenance of information systems' confidentiality and availability. We conducted this audit between January 2011 and April 2013 in accordance with generally accepted Government auditing standards. Exhibit A further details our scope and methodology.

BACKGROUND

AFS manages the Registry—located in Oklahoma City, Oklahoma—which consists of two databases, one on aircraft and the other on airmen. For aircraft, AFS accepts applications for and maintains permanent records on the registrations of all civil aircraft. Title 14 (Aeronautics and Space) of the Code of Federal Regulations (CFR) requires the application to include the aircraft's make, model, and serial number; the applicant's permanent address; and documentary proof—such as title of ownership or bill of sale—that the applicant owns the aircraft. Each applicant for registration must also certify that he or she is a citizen of the United States and that the aircraft is not registered under the laws of any other country. AFS reviews each applicant's information and issues Certificates of Aircraft Registration to applicants who meet requirements.[4]

FAA regulations also allow the registration of aircraft owned under trusts,[5] which allow non-U.S. citizens to have their aircraft registered on FAA's Registry. To do this, an aircraft owner will create a trust agreement that transfers the aircraft's title to an American trustee. The trustee, who may be an individual or organization, will register the aircraft under his/her or its name. The agreement will also identify the beneficiary or person who can use the aircraft. The owner and the beneficiary are frequently the same person.

In July 2010, to ensure that aircraft owners provide accurate information for Registry records, FAA issued a rule on aircraft re-registration[6] and registration renewal. The rule requires the re-registration of all civil aircraft by December 31, 2013, and enables FAA to cancel the registrations of aircraft that are not re-registered by this date. After initial re-registration, all aircraft registrations must be renewed every 3 years.

---

[4]Title 14, Section 47.5 of the CFR actually states that the Certificate of Aircraft Registration is issued "to the person who **appears** to be the owner" (emphasis added) of the aircraft.

[5]A trust is a legal entity created by one party, the owner and trustor, through which a second party, the trustee, holds the title to the trustor's assets or property for the benefit of a third party, the beneficiary. The trustor/owner may also be a trustee and/or one of the beneficiaries.

[6]Re-registration will take place between October 1, 2010, and December 31, 2013. All owners are required to re-register by predetermined quarterly dates based on the month of original registration. First-time registrations issued on or after October 1, 2010, also expire after 3 years.

CFR 14 also requires all persons who operate aircraft in the United States to obtain and maintain a valid pilot's certification. AFS accepts applications for pilots' certifications and maintains permanent records on the certifications in the Registry's pilot database. An application for a pilot's certification includes the applicant's social security number and date of birth, a record of pilot flight time, and the basis for the application such as test results or graduation from approved courses[7]. FAA uses designated examiners[8]—private individuals who act on FAA's behalf—to review and approve the applications, and AFS's Registry examiners review approved applications and issue certifications. FAA contracts with a vendor who furnishes the facilities, management, personnel, equipment, and materials necessary to produce and mail pilots' certifications.

RESULTS IN BRIEF

FAA's Civil Aviation Registry lacks accurate and complete information needed for aviation safety and security measures. The Registry lacks information on registered aircraft, owners—including non-U.S. citizens—and their compliance with FAA regulations. FAA's regulations require owners to periodically update or correct the information in their Registry records, but the Agency does not check these re-registrations against the original records to ensure accuracy and regulatory compliance. We found incomplete registrations for about 5,600 aircraft, or 54 percent, owned under trusts for non-U.S. citizens. As a result, FAA has been unable to provide information on these aircraft to foreign authorities upon request when U.S. registered aircraft are involved in accidents or incidents in foreign countries, as required by the Convention on International Aviation. FAA's Registry similarly lacks complete information on pilot certifications, which makes it difficult for law enforcement officials to use the Registry to conduct security screenings required by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) or to detect pilots who provide false information. These data weaknesses largely stem from FAA's lack of formal quality control procedures to regularly reassess the integrity of the Registry's data and information systems.

FAA has not implemented needed security controls over the Registry's configuration and account management to mitigate the risk of unauthorized access to PII. FAA maintains it is not responsible for information voluntarily submitted to the Registry. However, FAA's practices are contrary to Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) requirements that require protection of PII and emphasize the importance of access controls, up-to-date operating systems, and continuous monitoring. We found multiple weaknesses with the Registry servers, including outdated operating

[7]Submission of the data is mandatory, except for the Social Security Number, which is voluntary.
[8]Designated examiners exercise the authority of the FAA Administrator to certify and approve pilots' records, certifications, and test results.

systems and no routine monitoring over sensitive data access. FAA is also not in compliance with DOT policies calling for PII encryption and account access controls. Finally, FAA does not have agreements in place with external parties that receive registry information to protect PII to prevent unauthorized access, as required by the Federal Information Security Management Act (FISMA).

FAA's recovery plan for the Registry does not meet DOT's information technology (IT) security policy requirements and is inadequate to ensure that the system is recoverable after a disaster or other event causing it to be shut-down. For example, FAA's test procedures for the Registry's recovery plan did not include an alternative processing site for the resumption of Registry functions in case of a shut-down. Due to a reorganization of information technology activities some years ago and the Registry's complexity, FAA had not yet selected an alternate processing site. Lack of testing of the Registry's backup systems at an alternative site creates the risk that FAA will be unable to resume essential operations after a system shut-down.

We are making recommendations to improve the accuracy, security, and reliability of the Registry's data.

FAA'S REGISTRY DOES NOT CONTAIN COMPLETE AND ACCURATE INFORMATION ON AIRCRAFT REGISTRATIONS AND PILOT CERTIFICATIONS

FAA does not maintain accurate or complete information in its Registry. For example, it lacks information on registered aircraft, owners—including non-U.S. citizens—and their compliance with FAA regulations. FAA similarly lacks complete information on pilot certifications, which makes it difficult for the Transportation Security Administration (TSA) and other law enforcement officials to use the Registry for required security screenings or to detect pilots who provide false information. A major factor contributing to these weaknesses is FAA's lack of formal quality control procedures to regularly reassess the integrity of the Registry's data and information systems.

The Registry Lacks Complete and Reliable Information on Registered Aircraft and Their Owners and Operators

The Registry lacks information on registered aircraft, their owners, and their operators that FAA needs for aviation and security measures. We selected a random sample of 68 out of 10,292 fixed wing and rotary aircraft registrations and found that 37 out of 68 had incomplete registrations. Based on this finding we estimate that 5,600 or 54.4 percent of aircraft owned under trusts for non-US citizens lacked important information such as the identity of the trusts' owners and

aircraft operators.[9] While FAA's regulations require registration applications to include copies of all documents that establish these trusts, they require few documents that identify the owners who established the trusts and how the trusts comply with regulations. However, under the Convention on International Civil Aviation,[10] FAA has a duty to provide, upon request from appropriate foreign civil aviation authorities, accurate information on U.S. registered aircraft operated in foreign countries. Foreign aviation authorities have brought to FAA's attention numerous accidents, operational errors, and other incidents involving U.S. aircraft registered to trusts for non-U.S. citizen beneficiaries. Because the Registry lacks information on these aircraft, FAA is at risk of not being able to meet its duty under the Convention and answer these authorities' requests for information. FAA has taken actions by convening a working group to identify key issues, holding public meetings, and issued proposed policy clarification in the Federal Register for these types of aircraft registrations, but has yet to conclude work in this area. We are conducting additional audit work on the relationships between these trustees and the anonymous owners/beneficiaries.

We also found errors in Registry data. Specifically, 130 of 350,000 aircraft registration records in the Registry share make and model information and serial numbers with at least 1 other aircraft, making it difficult for FAA and other Registry users to identify the true owners of these specific aircraft. While this is a small number of discrepancies, the impact is potentially significant if a serious incident occurs and FAA is unable to identify the aircraft's owner in a timely manner. Inadequate quality control procedures contribute to such errors. For example, FAA does not check the Registry for duplicate information or perform semi-annual reassessments to review the information in aircraft registrations for accuracy or compliance with regulations in accordance with DOT policy.[11] Instead, FAA relies on each aircraft owner to validate that the information on his or her aircraft—including make, model, serial number, and the owner's physical address—in the Registry is current.

The Registry Does Not Contain Complete and Accurate Information on Pilots' Certifications

The Registry also lacks information on pilots that FAA needs to ensure aviation safety. Over 43,000 airmen have received certifications even though they have not provided FAA with accurate permanent personal addresses. Despite its policy,[12] FAA has permitted pilots to use business and flight school addresses on their

[9]Our 5,600 estimate has a precision of +/-1,027 at the 90-percent confidence level.
[10]Known as the Chicago Convention, it was signed on December 7, 1944.
[11]DOT Order 1351.37 Departmental Cybersecurity Policy requires that System Owners perform semi-annual reassessments of the integrity of information and ensure the validity of information inputs.
[12]FAA Order 8900.2 CHG 1, General Aviation Airman Designee Handbook.

applications for certification. As a result, it is difficult for TSA to locate individuals to conduct IRTPA-required pilot screening. These screenings must be complete before FAA can issue pilot certifications. The Government Accountability Office (GAO) recently reported on the impact that FAA's lack of data on pilots has on aviation safety[13] and has highlighted the importance of the Registry's accuracy for ensuring aviation security.[14]

FAA also does not comply with IRTPA's requirements for more secure pilot certification documentation. IRTPA requires FAA to issue pilots' licenses that are tamper resistant, include a photograph of the pilot, and can accommodate a biometric identifier, such as fingerprints. According to FAA officials, however, the Agency does not yet require pilots to provide photographs or biometric identifiers for inclusion in their certifications due to its lack of expertise in biometrics and a late start in its preparation to meet the requirement. The Department of Homeland Security's Inspector General has reported[15] that because FAA does not require unique identifiers—such as photographs or social security numbers—on pilots' certifications, TSA may not be able to identify pilots who provide false personal information on their certification applications thereby making it easier for individuals using false identities to receive certifications.

FAA Lacks Formal Quality Control Procedures for the Registry

FAA does not have formal quality control procedures to conduct regular integrity assessments of the Registry's data. DOT policy[16] states that Information System Owners—the manager responsible for an information system's operation and maintenance—must reassess semi-annually the integrity of both their systems' information and software. Furthermore, System Owners must ensure that their information systems validate information inputs to ensure that the systems' data are complete, accurate, and valid, and that the systems identify and reject any incorrect information. However, FAA has no documentation that describes the Registry's quality control requirements for reassessing its data and how those requirements correspond with FAA's policy and regulations.[17]

---

[13]GAO, Additional FAA Efforts Could Help Identify and Mitigate Safety Risks, GAO-13-36, October 4, 2012.
[14]GAO, TSA's Process for Ensuring Foreign Flight Students Do Not Pose a Security Risk Has Weaknesses, GAO-12-900T, July 18, 2012.
[15]DHS, Transportation Security Administration (TSA) Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures, OIG-11-96, July 2011.
[16]U.S. Department of Transportation, Departmental Cybersecurity Compendium, Supplement to DOT Order 1351.37, June 14, 2011.
[17]14 CFR § 47 (Aircraft Registration) and § 61, 63 and 65 (Airmen Certification).

THE REGISTRY'S SECURITY CONTROLS ARE INADEQUATE TO PROTECT THE REGISTRY'S PII FROM UNAUTHORIZED ACCESS

FAA's security controls for the Registry's system configuration and account management do not adequately protect the PII in the system. FAA's controls do not comply with DOT policies and put the system at risk for unauthorized access. Furthermore, FAA does not require the contractor who produces pilots' certifications to have the security controls required by FISMA and DOT policy in place.

FAA's Inadequate Security Controls Put the Registry's PII at Risk for Unauthorized Access

OMB requires all Federal agencies to implement the security controls necessary to prevent inappropriate access to, use, and disclosure of PII. Furthermore, NIST specifies the controls for high-impact systems,[18] such as the Registry. For example, NIST requires access controls, up-to-date operating systems[19] and patches,[20] and continuous monitoring. Pilots' certifications contain particularly sensitive PII, including social security numbers and personal medical information. Aircraft records submitted during the registration process may also contain PII inadvertently included by the registrant. However, FAA has not implemented security controls that will mitigate the risk of unauthorized access to the Registry's PII. We performed a vulnerability assessment[21] of Registry systems and noted the following weaknesses:

- Thirty computer servers, 70 percent, of the 42 that support the Registry, contained at least 1 high risk or critical vulnerability—a weakness in an information system that could be exploited for unauthorized access.

- Two servers were running operating systems that were outdated and therefore no longer receiving vendor support or patches.

- Seven servers were missing update patches from 2007 and subsequent years.

- Access to sensitive Registry data is not monitored.

Furthermore, we found that FAA did not effectively implement the following controls that are required by FISMA, OMB, or DOT policy:

---

[18]A system is considered high impact if its loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

[19]An operating system is the software that allows computer users to run applications with the hardware of a specific system. Microsoft Windows or Apple Computer's OS are examples of operating systems.

[20]Patches are software that fix problems with computer programs, including system vulnerabilities.

[21]A vulnerability assessment is a method of identifying weaknesses present in information technology systems by examining the current software versions and settings.

- **PII encryption.** FAA does not encrypt[22] Registry data, including PII, on pilots and sensitive information inadvertently submitted by owners for aircraft registrations. The lack of encryption makes reading PII easier when it is accessed by an unauthorized party or stolen. During the pilot certification and aircraft registration processes, FAA receives copies of sensitive information such as driver licenses and documents ancillary to trusts, which without encryption, is at an increased risk of exposure.

- **Annual user account validations[23] to identify, disable, and remove accounts are no longer in use.** FAA only sporadically validates the Registry's user accounts and does not document this validation. Untimely disabling and removal of accounts could lead to unauthorized access to information and systems by individuals who are no longer authorized. Additionally, FAA has inadequate policies and practices for creating and managing user accounts. For example, FAA's system access authorizations do not adequately segregate approval and recording of changes to user accounts.

- **Multifactor user identity authentication.** OMB requires multifactor identity authentication, which consists of a password and another access method such as a smart card, to verify Registry users' identities before granting system access. Although FAA indicated that the Registry uses digital signatures[24] to authenticate Registry users, we found that it does not use this technology or multifactor authentication. In addition, there are over 38,000 Registry users—designated examiners that certify pilots' certifications application—who are not FAA employees, heightening the need for strong access controls, such as multifactor identity authentication, to prevent compromise of pilots' PII.

Inadequate procedures, delayed resolution of identified weaknesses, and not accepting responsibility for PII voluntarily submitted to the Registry contributed to these weaknesses. Specifically, FAA had no written procedures and guidance on configuration management and changes making it difficult to monitor and patch the system. FAA also had not completed the corrective actions included in its plans of action and milestones (POA&Ms) to address identified weaknesses. Twenty-six POA&Ms, including high risk items that FAA identified in 2009, were not resolved in a timely manner. For example, FAA wrote a POA&M for its lack of a configuration management plan for the Registry's system with a completion date of May 31, 2010, but did not complete the plan until October 2011. Finally, FAA officials informed us that because PII in aircraft registration records are

[22]Encryption is the process of changing information in such a way as to make it unreadable by anyone except those possessing special knowledge (usually referred to as a "key") that allows them to change the information back to its original, readable form.

[23]Annual validation is required for users' accounts and semi-annual for system owners and administrators' accounts.

[24]Digital signature is a technology that uses encryption to authenticate the person who transmits information over a network and to ensure that the information is not changed during transmission.

voluntarily submitted to the Registry by aircraft owners, FAA does not have any responsibility to safeguard this sensitive information.

FAA Has Not Established Required Agreements with its Contractor and Other Agencies That Receive Registry Information to Ensure That Their Systems Protect the Information

FAA does not have FISMA-required agreements with its contractor and other Federal agencies that receive Registry information to ensure that these third-parties' systems can protect the Registry's PII from unauthorized access. FISMA requires Federal agencies to establish interconnection security agreements to authorize connections from one information system to systems outside of their authorization. These agreements provide assurance that the outside systems are secured according to the requirements for Federal information processing systems. DOT policy also calls for FAA to require providers of external information system services to employ security controls in accordance with the requirements for Federal systems. However, FAA has not entered into such an agreement with the vendor that produces pilots' certifications or included the required terms in its contract with the vendor. FAA also shares Registry information with other Government agencies, such as TSA, and Federal and State prisons, but does not have interconnection security agreements with all such entities. As a result, FAA does not have any assurance that the information it provides to external parties will be properly secured.

FAA'S CONTINGENCY PLAN FOR THE REGISTRY CANNOT ENSURE THAT THE AGENCY WILL RECOVER THE SYSTEM AFTER A SHUT-DOWN

FAA's contingency plan for the Registry does not ensure that FAA will be able to recover the Registry after a shut-down. At the time of our review, the plan described how to recover the system in the event of an emergency shut-down. However, FAA had not yet established an alternative operation site for the Registry. Both NIST Special Publication 800-53 and DOT policy, issued in August 2009 and June 2011 respectively, require DOT's operating administrations to establish alternate processing sites for their information systems and to implement plans for the resumption of system operations for essential missions and business functions when the primary processing capabilities are unavailable.

Furthermore, FAA's test procedures for the Registry's recovery plan do not include testing a recovered system. Because the Registry is a high-impact system, NIST requires FAA to test the Registry's contingency plan at the alternate processing site to determine the plan's effectiveness and staff's readiness to execute the plan, review the test results, and initiate corrective actions. However,

FAA only makes phone calls to ensure that the key personnel can be contacted in the event of an emergency shut-down of the Registry.

Due to a reorganization of information technology activities a number of years ago and the Registry's complexity, FAA is still working to establish the Registry's alternative processing site. However, the lack of testing of the Registry's backup systems at an alternative site creates the risk that FAA will be unable to resume essential operations after a system shut-down and ensure continued access to aircraft registrations and pilot certification records.

CONCLUSION

DOT's primary mission is safety. Integrally related to the safety of aviation operations is the security and integrity of information FAA collects on the pilots and aircraft operating in the National Airspace System and around the world. In furtherance of the aviation safety mission, FAA must collect and protect complete and accurate aircraft and pilot data. In addition, FAA must also ensure this data is readily available for safety purposes. The weaknesses we identified increase the risk that the integrity and privacy of the Registry's data will be compromised. In addition, in the event of a system disruption, the data may not be available in a timely manner. Until resolved, these weaknesses diminish FAA's ability to fully carry out its safety mission and provide required services and assistance to the aviation public, airlines, law enforcement, foreign governments, and Federal agencies responsible for homeland security.

RECOMMENDATIONS

To improve the accuracy, security, and reliability of the Registry's data, we recommend that FAA's Administrator require the Associate Administrator for Aviation Safety in consultation with the Agency's Chief Information Officer:

1. Develop procedures for periodic reassessments of aircraft and airman data to improve and maintain data integrity.

2. Issue policy or regulations that clarify informational requirements for registration of aircraft owned by trusts for non-citizens.

3. Develop procedures to ensure that airman addresses are kept current.

4. Implement the provisions of the Intelligence Reform and Terrorism Prevention Act's for pilot certifications.

5. Implement access monitoring, user accounts, and multi-factor authentication for the Registry.

6. Encrypt PII and mitigate the vulnerabilities on Registry computers. If controls cannot be implemented immediately then remove all PII or take other actions as appropriate, such as suspend the system's operation in accordance with FAA Order 1280.1B.

7. Ensure that the FAA contractor's computers and other third-party systems comply with information security controls required by FISMA and DOT policy.

8. Mitigate contingency planning weaknesses by selecting an alternative processing site and periodically conducting comprehensive contingency tests at the alternate site in accordance with DOT policy.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided FAA with a draft of this report on April 4, 2013, and requested the Agency's response within 30 calendar days. We received the response on June 20, 2013, which is included as an appendix to this report. FAA concurred with five of our eight recommendations (2, 3, 4, 7, and 8) and partially concurred with three (1, 5, and 6).

FAA concurred with recommendation 2 and requested that it be closed based on its recent publication of a revised policy on registration of non-citizen trusts; however, we do not agree that FAA's clarification of its aircraft registration policy will ensure that FAA has the information it needs. The new policy states that trustees, upon FAA's request, should provide information about registered aircraft and their operations within set time frames. However, FAA states that the Registry is the system of record in which the Agency maintains information that users need to locate individuals and aircraft. For the Registry to meet this purpose, FAA must collect this information as part of the registration process so that is available to users when they need it. Consequently, the new policy does not ensure that FAA will have the information it needs for proper safety oversight. Therefore, we request that FAA reconsider its response and provide information to clarify how it will collect and maintain current information about the ownership and operation of all aircraft owned under trusts for non-citizens.

FAA partially concurred with recommendations 1, 5 and 6. However, its planned actions do not address the recommendations' full intent. Therefore, we consider

them open and unresolved and request that FAA reconsider its related responses. Specifically:

- We disagree that the Agency has quality control processes in place that are sufficient to resolve recommendation 1. In addition, FAA has not provided information describing its quality control requirements for regular reassessments of the Registry's data. The Agency's planned action on data integrity improvements would be beneficial but does not go far enough. DOT policy requires semi-annual data integrity assessments for all information systems. FAA's planned action does not comply with this policy. Therefore, we request that FAA provide additional information on actions it plans to take to periodically reassess the Registry's data to identify and correct aircraft registrations and pilot certifications that do not conform to its policies and regulations.

- In response to recommendation 5, FAA stated that its self assessments of the Registry determined that the Registry's system was at low risk for inadvertent disclosure of sensitive information, despite the fact that FAA has not implemented system account management and strong user identity authentication mechanisms. Further, FAA categorized the Registry as a high impact system, meaning that loss of confidentiality, integrity or availability of its information would have a severe or catastrophic effect on FAA's operations. DOT policy requires high impact systems to use annual account validations and multifactor identity authentication to protect their sensitive information. FAA's response does meet these DOT policy requirements for such high risk systems. Therefore, we request that FAA provide clarifying information on its plans for establishing annual account validations and multifactor user identity authentication.

- FAA's lack of encryption of the data on its legacy systems does not comply with DOT policy and, therefore, does not sufficiently address recommendation 6. DOT policy requires encryption of all sensitive PII, wherever it may reside, and does not allow for application of encryption when practical. We request that FAA provide information on its planned action to include encryption of all sensitive PII in the Registry, including that contained in legacy systems.

Given FAA's reaction to our recommendations, we remain concerned that the integrity and privacy of the Registry's data will remain at risk.

ACTIONS REQUIRED

FAA's planned actions for recommendations 3, 4, 7, and 8 are responsive and we consider these recommendations resolved but open pending completion of the

planned actions. For recommendations 1, 2, 5, and 6, we are requesting the Agency provide additional information on its planned actions, as detailed above. In accordance with DOT Order 8000.1C, we request this information within 60 days. All corrections are subject to follow-up provisions in DOT Order 8000.1C.

We appreciate the courtesies and cooperation of Federal Aviation Administration representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407, or Joann Adam, Program Director, at (202) 366-1488.

#

cc: Chief Information Officer, DOT
Associate Administrator for Aviation Safety, FAA
Assistant Administrator for Information Services and
Chief Information Officer, FAA
DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted our work from January 2011 through April 2013 in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To determine the sufficiency of the Registry's aircraft registrations and pilots records, if PII was secure from unauthorized use or access, and if contingency planning ensures Registry continuity, we interviewed officials from several FAA offices and directorates. This included FAA's Flight Standards Service–Civil Aviation Registry and Flight Standards Division Special Emphasis Investigations Team. We also interviewed officials from FAA's Office of Quality, Integration, and Executive Services; Office of the Chief Counsel; Office of Information Services–Information Systems Security; and Office of Acquisition Services–Contract Management Team. We obtained, reviewed, and analyzed documentation related to the confidentiality, integrity, and availability of the FAA's Registry system.

We used a statistical sample of 68 aircraft out of 10,292 from the Registry to evaluate aircraft registration compliance with 14 CFR § 47 (Aircraft Registration). We tested five key registration requirements on each of the 68 aircraft for a total of 340 tests. This statistical sample allowed us to project aircraft registration errors with a 90 percent confidence level and a precision of +/- 10 percent.

Finally, we performed a vulnerability assessment of the Registry's Pilot and Aircraft system components, including Pilot/Aircraft Web Services, IACRA Web Services and Admin web site, Electronic Document Retrieval System (EDRSII), Image Management System and the Registry and Office of Aviation Safety data center's pilot and aircraft processing infrastructure. We performed the assessment using automated software tools as well as manual testing techniques. The results of the scans were reviewed to determine if security settings meet policy and baseline requirements for security testing, vendor updates (patches), and FAA's configuration of these systems.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Joann Adam	Program Director
Gerald Steere	Project Manager
Tim Roberts	Senior Auditor
Maria Dowds	Senior Auditor
Susan Neill	Writer-Editor
Seth Kaufman	Senior Counsel
Sandra DeLost	Information Technology Specialist
Megha Joshipura	Statistician
Petra Swartzlander	Senior Statistician
Allison La Vay	Referencer

Federal Aviation Administration

Memorandum

Date: June 20, 2013

To: Louis C. King, Assistant Inspector General for Financial and Information Technology Audits

From: H. Clayton Foushee, Director, Office of Audit and Evaluation, AAE-1

Subject: Federal Aviation Administration's (FAA) Response to Office of Inspector General (OIG) Draft Report: FAA's Civil Aviation Registry

The FAA Civil Aviation Registry (Registry) manages the permanent records for aircraft registration and airman certification. Each is governed by a Systems of Record Notice establishing its purpose, scope, and routine uses. Both systems are constantly evolving with changes in the industry and regulatory environment. Improvements in data quality, error checking, appropriate user access, and security are continually evaluated through International Organization for Standardization (ISO-9001) certified processes and advances in automation technologies.

RECOMMENDATIONS AND RESPONSES

Recommendation #1: Develop procedures for periodic reassessments of aircraft and airman data to improve and maintain data integrity.

Response: Partial Concur. As described in the draft report, the Registry already has processes in place to review aircraft and airman records, as well as quality control processes. The FAA does not believe the recommended establishment of a scheduled periodic reassessment procedure offers sufficient improvement to be worth the investment in resources that would be required. However, the Registry will evaluate ways to improve data quality and integrity and provide a follow-up response by December 31, 2013.

Recommendation #2: Issue policy or regulations that clarify informational requirements for registration of aircraft owned by trusts for non-citizens.

Response: Concur. An official FAA policy clarification on registration of aircraft owned by trusts for non-citizens has been under development since early 2010 and was

published in the Federal Register on June 18, 2013. The FAA request this recommendation be closed.

Recommendation #3: Develop procedures to ensure that airman addresses are kept current.

Response: Concur. Airmen are required by 14 Code of Federal Registration Part 61.60 to report a change in address within 30 days of a move and must provide an acceptable physical residential address if different than a mailing address. It's the responsibility of the airman to inform the FAA if there is a change of address, and this can be accomplished through a change of address notification, when adding a rating or applying for an airman certificate or replacement. The FAA provides policy guidance regarding acceptable address information for FAA authorized designees, FAA inspectors and other officials in FAA Orders 8900.1, 8900.2 and other publications. Additional instructions are provided on each application for an airman certificate and/or rating. If an airman/applicant provides an unacceptable address, the Registry rejects the application or request for reissuance of a certificate and the permanent airman certificate is not issued until the airman complies with the FAA address requirements to provide an acceptable address. Currently, the FAA does not preclude an airman from using a flight school address or acceptable commercial address as a preferred mailing address, as long as the airman also provides an acceptable physical, residential address for the official airman record. Both addresses, when provided, are included in data that the FAA provides to the Transportation Security Administration (TSA) and other law enforcement entities, as required by U.S.C. 44703. The residential address may be shown in the database or contained within the airman record on digital images.

Also, the FAA continues to update its system to identify addresses that are not acceptable in accordance with U.S.C. 44703, and has implemented software changes and system edits to identify unacceptable addresses. The Registry utilizes United States Postal Service software to identify and standardize address information in order to ensure the address information provided by an applicant is not a fictitious address and to ensure proper delivery of the airman certificate. Going forward, the FAA has purchased new address validation software, called Melissa Data, which is currently undergoing testing to confirm that it will identify a "commercial" address (such as a flight school address), which would thereby require the airman to provide a physical residential address for official record purposes. If this testing is successful, the FAA plans to fully implement Melissa Data by September 30, 2014 and will also purchase a subscription of annual updates to ensure continuing currency of address validation data.

It should be noted that many of the records identified by the OIG were established prior to the requirement to provide a physical residential address. These airmen have had no other contact with FAA, in some cases, since the original issuance of the airman certificates. Many of the airmen the OIG identified are not “active”, and many of the airman certificates were issued before or during the 1970’s and 1980’s, prior to the requirement to provide a physical residential address (DEA Act of 1988). Prior to 1988,

it was acceptable to use an aviation school address, a post office box or other mailing address when applying for an airman certificate and the purpose of capturing an address was to ensure the FAA had a good address to be able to mail airman certificates, FAA safety publications and notices to airmen.

Recommendation #4: Implement the provisions of the Intelligence Reform and Terrorism Prevention Act's (IRTPA) for pilot certifications.

Response: Concur. Historically, the purpose of a pilot certificate is to display airman certificate privileges and qualifications. Section 4022 of IRTPA changed the purpose and utilization of a pilot certificate and required the FAA to issue improved pilot certificates that (1) are resistant to tampering, altering, or counterfeiting; (2) include a photograph of the individual to whom the certificate is issued; and (3) are capable of accommodating a digital photograph, a biometric identifier, or any other unique identifier that the FAA Administrator considers necessary.

The FAA began issuing plastic tamper- and counterfeit- resistant certificates in 2003. In February 2008, the FAA published the Drug Enforcement Assistance (DEA) final rule (73 FR 10662), which required all pilots (except student pilots) to obtain the tamper-resistant plastic certificate by March 31, 2010. The DEA final rule satisfied the IRTPA requirement to issue pilot certificates that are resistant to tampering, altering and counterfeiting.

In November 2010, the FAA published a Notice of Proposed Rulemaking (NPRM) titled "Photo Requirements for Pilot Certificates" (75 FR 70871). The NPRM proposed to fulfill the final requirements of section 4022 of the IRTPA by requiring a photo of the pilot on all plastic pilot certificates, including students. This rulemaking project was placed on hold because it was superseded by Section 321 of the FAA Modernization and Reform Act of 2012. To address the additional requirements of Section 321, and because a pilot certificate is not and has never been utilized as a security credential, the FAA formed a working group consisting of multiple FAA and TSA offices. This working group is evaluating the FAA's current certification processes and how they could be changed to accommodate such certificates, the infrastructure required to utilize such certificates, and associated costs that may be incurred. For example, the FAA must consider infrastructure requirements such as biometric collection and card readers that would need to be developed and distributed for airmen, government and industry to utilize biometric pilot certificates. The working group is also looking at funding considerations, and options to reduce the burden on the public and the FAA.

The new associated rulemaking project has been accepted by FAA's Office of Rulemaking, but a schedule has not yet been approved. The timing of any proposed rule will be critical so as not to duplicate rulemaking efforts between TSA and the FAA, but the complex project is unlikely to be complete in the near term, and therefore the FAA will provide an update by September 30, 2015.

Recommendation #5: Implement access monitoring, user accounts, and multi-factor authentication for the Registry.

Response: Partial Concur. The FAA concurs with the recommendation to implement access monitoring but does not concur with the recommendations regarding user accounts or multi-factor authentication.

The OIG conducted this audit between January 2011 and April 2013. During this period, the FAA closed a number of open Plan of Action and Milestones (POA&M) items which add insight into FAA's activities on this issue. The OIG confirmed the Fiscal Year (FY) 2012 Assessment Team audit review finding Cyber Security Assessment and Management ID 48954) that web application audit logs are not routinely monitored. During the follow on FY2013 assessment, the Assessment Team concluded that the system owners review web application audit records on a daily basis, and recommended closing POA&M item 48954 with an effective date of March 2013. The FY2013 Assessment Team also recommended that the Integrated Airman Certification and Rating Application (IACRA) Information Technology Program Manager continue progress on POA&M item 28838, to modify the application to have a user interface that can display audit reports such as events that occurred during a selected time span or a listing of audit records for a specific event type. This modification is scheduled to be completed by September 30, 2013.

The OIG proposes an annual process to validate user accounts for the Registry web applications and the IACRA system. These applications provide services to authorized users, as the user requires these services, but once authorized, the applications do not require any minimum level of activity to maintain an account. The FY2013 Security Assessment Team assessed this risk as the lowest level of risk that can be calculated for the Registry system. Based on the business requirements and the extremely low risk, the Assessment Team recommended that the risk be accepted by the Authorizing Official, as it was previously with POA&M item 38397.

The Office of Management and Budget published Memorandum number 4 in FY2004 (M-04-04) that describes the e-authentication analysis process. Assessment Teams use the M-04-04 process to determine the level of authentication required for non-organizational (external) users, e.g. Designated Pilot Examiners. The IACRA system and the Registry web applications authenticate external users. The FY2013 Assessment Team completed independent assessments and determined that level 2 user identifier and passwords are appropriate and should be required. The FAA reviewed, and concurs with the Assessment Team conclusion, that multi-factor authentication is not required for external users.

Recommendation #6: Encrypt PII and mitigate the vulnerabilities on Registry computers. If controls cannot be implemented immediately then remove all PII or take other actions as appropriate, such as suspend the system's operation in accordance with FAA Order 1280.1B.

Response: Partial Concur**.** The FAA concurs with the OIG recommendation to mitigate the vulnerabilities on the Registry computers. However, this remediation cannot be

performed immediately. FAA Order 1280.1B, *Protecting Personally Identifiable Information (PII),* does not require immediate implementation and thus the FAA will not suspend operations. The Registry and IACRA systems will continue to operate while the FAA performs activities to mitigate the vulnerabilities.

The OIG confirmed the FY2012 Assessment Team patch management finding. In response to missing patches, the FY2013 Assessment Team updated POA&M item 38344 for the Registry and developed a new POA&M item for the IACRA system to address missing security patches. The FAA concurs with the OIG conclusions and assessed these POA&M items at a high risk level. Remediation is scheduled for completion by September 30, 2013.

As the OIG noted in the findings, the Registry system contains several legacy components, therefore, the FAA will not be able to encrypt all PII. In cases where encryption is not practical, the FAA will continue to implement strong access controls to PII in accordance with DOT Privacy Policy. The current access controls reduce risk to an acceptable level, in compliance with that same DOT Privacy Policy.

It is not practical to implement encryption in the mainframe portion of the Registry system as this component is being phased out. In addition, the image files cannot be encrypted because of the legacy application. However, the image files are stored with a proprietary wrapper and are not directly readable from storage. The sensitive data residing in databases in the enterprise data center can be encrypted, and the FAA is reviewing potential solutions and plan to implement by December 31, 2013.

Recommendation #7: Ensure that the FAA contractor's computers and other third-party systems comply with information security controls required by FISMA and DOT policy.

Response: Concur. The FAA will add additional security controls to the next contract and Statement of Work (SOW) which goes into effect October 2013. Even though specific security requirements were not listed in the contract, the security requirements were vetted by the FAA's contracting office prior to awarding the contract. The current SOW requires periodic background checks on each individual with access to airman data and the contractor routinely provides background check results to the FAA.

Recommendation #8: Mitigate contingency planning weaknesses by selecting an alternative processing site and periodically conducting comprehensive contingency tests at the alternate site in accordance with DOT policy.

Response: Concur. An alternate data center with demonstrated failover capability has been an identified vulnerability (POA&M item 48951). Due to competing priorities, slow progress has been made with a tentative date of September 30, 2014 to remediate this vulnerability. The FAA plans system functionality testing at the FAA disaster recovery site, the William J. Hughes Technical Center (WJHTC), Atlantic City, New Jersey. This activity is dependent upon the Unisys upgrade to version 8.2 and the

inclusion of the ancillary servers on the replication platform. The FAA scheduled this item to be completed by September 30, 2014.

Although the FAA still needs to conduct functional testing at the alternative processing site, the FAA has conducted several other contingency tests. The Registry has an approved Information Security Contingency Plan in place in which Registry data is transferred to the WJHTC to provide an offsite storage location that is not subject to the same hazards as the primary site. The FAA has successfully completed file recovery exercises of the data transferred to the WJHTC. Additionally;

1. The FAA participates in two exercises per year simulating the loss of the mainframe component and also participates in the Mike Monroney Aeronautical Center exercises to evaluate continuity of operations readiness in a variety of scenarios.
2. Offsite backups and multiple levels of data protection are already in place. However, providing an alternate datacenter with demonstrated failover capability has been an identified vulnerability and the FAA plans to remediate this vulnerability by September 30, 2014.
3. System functionality testing is scheduled to be done at the designated Aviation Safety disaster recovery site at Atlantic City, New Jersey. This activity is currently scheduled to be completed by September 30, 2014.