

**INFORMATION SECURITY AND
PRIVACY CONTROLS OVER
THE AIRMEN MEDICAL SUPPORT SYSTEMS**

Federal Aviation Administration

Report Number: FI-2010-069

Date Issued: June 18, 2010



Memorandum

U.S. Department of
Transportation

Office of the Secretary
of Transportation
Office of Inspector General

Subject: **ACTION:** Report on Information Security and
Privacy Controls over the Airmen Medical Support
Systems
Federal Aviation Administration
Report Number FI-2010-069

Date: June 18, 2010

From: Rebecca C. Leng *Rebecca Leng*
Assistant Inspector General for Financial and
Information Technology Audits

Reply to
Attn. of: JA-20

To: Associate Administrator for Aviation Safety, FAA

This report presents the results of our review of the information security and privacy controls over the Federal Aviation Administration's (FAA) Airmen Medical Support Systems (MSS). FAA requires airmen to hold a medical certification of their medical and mental fitness to operate aircraft.¹ MSS currently stores more than 18 million medical records supporting the medical assessment of over three (3) million airmen. To ensure aviation safety and protect the privacy of airmen, it is critical that this medical information be secure. Also, coordination with other Federal agencies may improve aviation safety by identifying airmen who are receiving disability benefits and may not have disclosed potentially disqualifying medical conditions.

This review was requested by the Chairmen of the House Committee on Transportation and Infrastructure and its Subcommittee on Aviation. The objectives of our audit were to (1) determine if airmen's personally identifiable information (PII) is properly secured from unauthorized use or access, and (2) assess FAA's progress in establishing mechanisms to identify airmen holding current medical certificates while receiving disability pay.

To conduct our work, we interviewed officials from FAA's Civil Aerospace Medical Institute located in Oklahoma City, Oklahoma; FAA's Headquarters in

¹ A medical certificate must be held when exercising any of the following privileges: airline transport pilot, commercial pilot, private pilot, recreational pilot, flight instructor, flight engineer, flight navigator, or student pilot. Except for a person employed by FAA, a branch of the military services or the Coast Guard, a person acting as an air traffic control tower operator must also hold a medical certificate.

Washington, D.C.; as well as representatives from FAA's contractor and Aviation Medical Examiners' (AME) private medical support staff at various locations. We also spoke with officials from FAA's Office of Budget Policy Division. In addition, we performed a vulnerability assessment of the MSS network infrastructure, servers, Web applications, databases, and data interfaces. We conducted this audit between March 2008 and January 2010 in accordance with generally accepted government auditing standards. A detailed description of the scope and methodology used on this audit can be found in exhibit A.

RESULTS IN BRIEF

The names, addresses, Social Security numbers, medical data, and other PII of airmen are not properly secured to prevent unauthorized access and use. We found serious security lapses in FAA's management of AMEs private medical support staff access to the system. For example, medical examiners' former staff continued to have access to MSS. At the same time, FAA has not fully implemented security controls required by the Office of Management and Budget (OMB) and the Department to protect PII, such as multi-factor user authentication, audit trail reports to detect inappropriate access, and data encryption. In addition, FAA has not ensured secure configuration of MSS computers in accordance with the Department's baseline standards to reduce the risk of unauthorized access and corruption. Specifically, we found vulnerabilities on MSS computers, such as configuration allowing intruders to install malicious codes on FAA user computers. Inadequate contingency planning also threatens the service continuity of MSS. Combined, these weaknesses make airmen's PII vulnerable to unauthorized access and use and potential falsification of medical certificates that could lead to unfit airmen being medically certified to fly. During the course of our review, FAA took immediate action to enhance security protection by working with doctors to remove thousands of separated medical staff's access to MSS and retracting millions of PII records from the contractor's site. However, additional improvements are needed to adequately secure PII data from unauthorized use.

FAA has made limited progress in identifying airmen who receive disability benefits while holding medical certificates. While FAA has a draft matching agreement with the Social Security Administration (SSA) to reconcile data in MSS and SSA's disability benefits system, it has yet to establish a target date for completing the interface. Further, FAA has yet to coordinate with other benefits providers, such as the Department of Veterans Affairs and the Department of Labor. FAA continues to rely on airmen to disclose potentially disqualifying conditions when applying for medical certificates. FAA recently announced a onetime, limited opportunity for airmen to reveal previously undisclosed depression and use of antidepressant medications without being subject to FAA

enforcement action.² This step, however, does not take the place of a comprehensive approach to undisclosed medical conditions. Accordingly, FAA needs to expedite computer matching agreements with disability benefits providers, implement the checks under those agreements, and take appropriate enforcement action where falsifications are found.

To assist FAA, we are making a series of recommendations to strengthen the confidentiality, integrity, and availability of airmen PII and to ensure unqualified airmen do not receive a medical certification enabling them to fly.

BACKGROUND

MSS contains over 18 million medical records on more than 3 million airmen, of which over 465,000 have current medical certifications.³ In addition to medical information, the system contains other sensitive personal information, such as name, address, date of birth, and Social Security number of airmen. MSS is accessible to about 9,000 users, 8,500 of whom are AME—private physicians who function as FAA designees—or their staff, who enter the medical data into the MSS Web site on the Internet. AMEs and their staff have access to all information (including medical data) stored in MSS on airmen examined in their offices. In addition, they can access the name, address, date of birth, and partial Social Security number on all airmen examined by other AMEs and stored in MSS. Almost 300 AMEs reside in 89 foreign countries and conduct exams on airmen seeking to fly in the United States.

In 2007, the Inspector General testified before the House Committee on Transportation and Infrastructure that some airmen failed to disclose to FAA any medically disqualifying information on their applications for medical certificates. Further, some airmen held current medical certificates while simultaneously receiving disability benefits for medically disabling conditions.⁴ Our testimony suggested that FAA work with the SSA and other disability benefits providers to expeditiously develop and implement a strategy to check for and take appropriate certificate regulatory enforcement action where falsifications are found, and to consider revising its application for the medical certificate to require applicants to explicitly identify whether they are receiving medical disability benefits.

² 75 Fed. Reg. 17049 (April 5, 2010).

³ FAA's Civil Aerospace Medical Institute in Oklahoma City processes medical certificate applications in MSS.

⁴ Falsification of FAA Airman Medical Certificate Applications by Disability Recipients (CC-2007-063, July 17, 2007). OIG reports and testimony can be found on our Web page: www.oig.dot.gov.

SENSITIVE AIRMAN MEDICAL RECORDS ARE NOT PROPERLY SECURED FROM UNAUTHORIZED USE

DOT policy requires FAA to implement controls for removing medical record access rights when they are no longer required, to ensure user access is derived from a role-based validation process and each user's level of access is commensurate with a need to know, and to document all users who have access to sensitive data.⁵ However, such controls have not been implemented in MSS. At the same time, FAA has not implemented OMB guidance to secure PII in an automated information system or to properly configure MSS production and development computers to reduce the risk of tampering.

Medical Staff and Contractor Access Continued Despite A Need To Know

We contacted six AME physicians and medical staff with user access to MSS and found that, while all six were no longer employed with the AME, their MSS access status remained active, giving them easy access into the system to obtain sensitive PII or tamper with MSS data—including the potential to falsify medical certifications. In addition, AMEs and their staff—current and former—can access information on airmen who are deceased or inactive that comprise as much as 86 percent of airmen in the database (see table 1). While FAA uses such historical medical data on airmen as a valuable research tool, it provided no justification for keeping these records in the online database accessible by non-FAA personnel over the Internet.

Table 1. Schedule of Airman Records

	Medical Certifications		Medical Records	
	Number	Percent	Number	Percent
Active airmen	465,493	14%	5,145,075	28%
Inactive airmen	2,813,373	86%	13,336,748	72%
Total	3,278,866	100%	18,481,823	100%

In addition, FAA had been sending millions of airman medical records from the MSS database to its contractor's facilities, a practice that has been in place over the past decade. FAA's contractor has been using this live data in its system testing procedures, but FAA had not justified the contractor's need for using millions of live records—or considered the security implications of storing airman

⁵ DOT Information Technology and Information Assurance Policy Number 2006-22 – October 11, 2006 (revision 1): Implementation of DOT's Protection of Sensitive Personally Identifiable Information (SPII).

PII at the contractor facility. After we requested documentation of support and approval of the data transference, FAA concluded there was no business need to maintain the data at the contractor's site. Millions of PII records were purged from the contractor's site.

The control weaknesses we identified are largely the result of FAA's failure to provide adequate oversight of the contract by communicating the DOT requirements regarding access controls. Upon learning of these control weaknesses, we notified FAA, which responded in June 2009 (see Appendix A), stating that it had begun implementing corrective actions, such as working with doctors to remove access for separated medical staff. In addition, FAA purged millions of PII records from the contractor's site. However, the lack of documentation about the application security features such as definitions of users' ability to access data and perform critical functions continues to weaken FAA's ability to administer effective security.

MSS Does Not Comply with Department Guidance/Policy on Measures to Deter and Detect Unauthorized Access

In 2006, OMB reemphasized to agencies their responsibilities and corresponding policy to appropriately safeguard PII, such as implementing secure authentication methods for remote access to compensate for a lack of physical security controls.⁶ Following OMB's guidance, the Department required its operating components to encrypt PII data, use multifactor user authentication and DOT's Secure Remote Access (SRA) portal for remote PII access⁷, provide security and privacy awareness training for the AME users, and report abuses of access privileges. The Department issued their requirements in 2006; however, FAA has not fully complied with OMB and DOT requirements.

Data Encryption, Multifactor Authentication and Secure Remote Access

DOT requires operating components to encrypt all sensitive PII. At the time the policy was issued, DOT required all existing sensitive PII to be encrypted within 6 months. However, sensitive airmen information continues to lack encryption. MSS passwords were also stored in clear text on the system, thus lacking technical safeguards in accordance with existing DOT policy and the Privacy Act to ensure the security and confidentiality of privacy records and to protect against security threats. In addition, airmen's PII shared with another FAA system is not encrypted during transmission or when stored in the receiving system. FAA also lacks a written plan describing the required security and processing procedures for the interface.

⁶ OMB Bulletin M-06-16, "Protection of Sensitive Agency Information," June 23, 2006. OMB recommended controls to compensate for the lack of physical security when information is removed from, or accessed from outside the agency location.

⁷ DOT policy requires that all DOT personnel and contractors that access DOT internal networks and systems remotely shall use only an authorized and approved SRA.

FAA has also failed to implement strong mechanisms to authenticate users for remote access to MSS, as required by DOT policy and identified in FAA's MSS Information System Security Plan (ISSP). Specifically, the ISSP calls for MSS to comply with the National Institute of Standards and Technology's (NIST) level 4 technical requirements for multifactor authentication.⁸ Level 4—NIST's highest remote network authentication level—requires employment of at least two of the following three authentication methods: (1) a password or personal identification number; (2) a smartcard, badge, or other authentication token; and (3) a physical characteristic such as biometric information. While FAA has implemented password controls for MSS user authentication, we found no evidence that the required second authentication has been designed, tested, or implemented.

Further, FAA does not require remote users to go through the Department's SRA portal to access sensitive MSS information. The portal ensures user computers are appropriately configured with security updates and virus protection before access is granted to reduce the risk of attacks on departmental networks. Approximately 8,500 of MSS active users can access sensitive PII remotely without using the SRA portal.

Failure to encrypt sensitive PII and control remote access to MSS places airmen at unnecessary risk of identity theft, jeopardizes the integrity of the medical certification process, and increases risks of attacks on departmental networks.

Security and Privacy Awareness Training for AMEs and Their Staff

OMB Circular A-130, the Federal Information Security Management Act (FISMA), and the Computer Security Act of 1987 require agencies to ensure that all users of Federal computer systems are appropriately trained in policies and procedures regarding computer security, protection of privacy, as well as how to fulfill their security responsibilities before allowing access to the systems. Further, individuals are required to exhibit behavior consistent with the rules of the system and periodic refresher training for continued access.

Despite these requirements, which are part of DOT policy, FAA exempted AME staff from taking DOT's mandatory security awareness and privacy awareness training. FAA concluded that because the 8,500 AME users with access to MSS are identified as "designees," they are not required to take the mandatory training for employees and contractors. FAA also exempted AME staff from signing a "rules of behavior" agreement—an agreement that acknowledges responsibility to take all appropriate precautions to safeguard PII. FAA planned to include rules of behavior agreements in the Aviation Medical Examiner certification process once the agreement form is incorporated in the online MSS certification system.

⁸ NIST Special Publication 800-63 "Electronic Authentication Guideline".

However, 2 years have elapsed since FAA made this decision, and the full online system component has not yet been developed.

Without providing the required security and privacy training and receiving signed rules of behavior agreements, users of FAA's systems may fail to understand their responsibilities and adhere to practices for properly safeguarding sensitive data and all other Government owned information technology resources.

Management Reports and Other Controls to Identify Potential Inappropriate Access and Data Integrity Issues

MSS lacks audit trail reporting and accountability controls to detect incidents of staff abusing access privileges. Security testing conducted by FAA in September 2008 concluded that there are no audit trail reports to monitor and detect inappropriate user access. For example, while AME staff is authorized to access airmen PII to conduct medical examination, excessive access for personal reasons is not appropriate and needs to be deterred. This security testing resulted in recommendations that FAA implement a process to monitor user activities. Such controls have proven to be effective in detecting inappropriate access. For example, a State Department audit trail review found that personnel had inappropriately accessed Presidential candidates' passport information during the 2008 election. Like the State Department's passport system, MSS also contains sensitive information concerning well-known political leaders and other public figures.

Further, data extracts of sensitive airmen PII sent to other FAA systems are not logged or confirmed to have been deleted after 90 days, as required by departmental policy. FAA plans to implement the recommended audit and accountability controls by April 2010. However, while FAA has held internal discussions to address these weaknesses, it has not made progress on a solution due to consideration of a commercial "off-the-shelf" program to address audit, accountability, and logging at an enterprise level.

In addition, FAA has not implemented controls to validate critical data as it is entered into MSS. As a result, inaccuracies, such as invalid Social Security numbers, can be created when identifying airmen and interfacing data between various information systems. Inaccuracies in the MSS data could complicate the procedures to be used in a matching program with benefits provider data. As FAA moves closer toward performing a matching of airman data with disability benefits, it will be important to ensure it has the most complete, accurate, and valid information available in which to perform the computer matching.

NIST provides mandatory controls for Federal information systems, which require checks for completeness, accuracy, validity, and authenticity of information as close to the point of origin as possible. Without MSS data validations in place and

functioning, there is a risk that incomplete and/or inaccurate medical information could enter the MSS system impeding the efforts of investigators, aviation medical examiners, and other decision makers.

MSS Production and Development Computers Are Not Properly Configured to Reduce Risk of Unauthorized Access and Attacks

Web applications, databases, and other MSS system components were not properly configured, or patched with vendor upgrades, to reduce the risk of unauthorized access or sabotage. We found critical vulnerabilities in these components. For example, Web applications can be exploited to gain access to MSS, making FAA-user computers vulnerable to hacking and malicious codes. Vulnerabilities in the database allowed us to gain unauthorized access to MSS. Specifically, we were able to gain valuable configuration information—such as the database schema—by exploiting database passwords, which were both short and easy to guess because they were the same as user IDs.⁹

Our prior audit work as well as FAA testing identified additional security configuration issues. First, we noted that users are allowed six unsuccessful login attempts to the Web before the account is locked. The MSS ISSP requires unsuccessful login attempts to be limited to three. Second, the application does not have a session timeout after 15 minutes of inactivity.

These vulnerabilities are largely the result of weaknesses in the MSS change management process. Specifically, the process does not provide for assessments of the impact that planned system changes may have on security prior to implementation. For example, while FAA's processing checklist for system changes requires a review of previous Certification and Accreditation documentation, it does not require additional security testing that would identify new vulnerabilities introduced as a result of these changes. FAA is required by DOT policy to implement controls that provide for ongoing assessments of system security, which include monitoring changes to ensure security features remain in effect and are still functioning properly after system changes. FAA has only recently begun devoting the resources necessary to implement these controls.

Contingency Planning Weaknesses Threaten Service Continuity

FISMA requires Federal agencies to follow NIST standards for ensuring system continuity, which include contingency plan exercises and training, designating an alternate processing site, and system recovery capability. FAA designated MSS as a system which, if nonfunctional, has a high-risk impact on FAA missions. However, continuity controls for MSS did not meet NIST continuity standards for

⁹ The results of our tests were provided to FAA for remediation. FAA took action to correct weak front end application passwords during our review. However, our unauthorized access was possible because back end computers were not properly configured to meet security standards.

systems with a moderate-risk impact. For example, in lieu of a live recovery test, a MSS contingency plan exercise consisted of a single test—calls to key personnel to confirm contact phone numbers were correct. FAA could expand the scope and objectives of the exercise to include validating the content of the plan and related policies and procedures, as well as validating the participant's roles and interdependencies. In addition, FAA lacks a Memorandum of Understanding with the identified alternate processing site.

Several conditions put MSS at high risk of interruption. First, MSS has been operating on a back-up server since April 2008 when the primary server failed. However, FAA never replaced the back-up server. In addition, the MSS database version in production is no longer supported by the vendor, and only one Database Administrator (DBA) is working on the MSS system. As a result, security updates are not being issued to secure the current MSS database, and there is no backup personnel should the DBA become unavailable.

While FAA is aware of these issues, it has focused on meeting other MSS business requirements, such as implementing the MedXPress Web site—not on remediating service continuity weaknesses. Absent effective controls to ensure MSS system continuity, FAA may be unable to meet its statutory obligation to certify the health of pilots, air traffic controllers, and other FAA covered positions if the current system fails.

FAA HAS MADE LIMITED PROGRESS IN DETECTING AIRMEN RECEIVING DISABILITY BENEFITS WHILE HOLDING MEDICAL CERTIFICATES

To identify airmen who receive disability pay while holding medical certificates, FAA has conducted educational outreach, primarily by revising its medical certificate application forms and has worked with the SSA to discuss a computer matching agreement.¹⁰ However, the progress has been slow in developing and implementing mechanisms to systematically detect airmen applying for or holding medical certificates while receiving disability benefits.

FAA has taken productive steps toward educating airmen and AMEs of their responsibilities in ensuring airmen, who have disqualifying medical conditions, do not hold medical certificates. In September 2008, FAA revised the paper and Web site version of its Application for Medical Certification, Form 8500-8. The applications now include a question asking airmen to confirm whether or not they currently receive, or have ever received, medical disability benefits. These

¹⁰ Computer Matching Agreements are governed by 5 U.S.C. § 552a, Records maintained on individuals. No record that is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency.

changes serve to start a dialog between the AME and the airman about potentially disqualifying medical conditions related to disabilities and provide the basis for the AME to evaluate airman fitness while medical benefits are received. FAA also used its Web site and the Federal Air Surgeon's Medical Bulletin to educate AMEs on their responsibility to perform good examinations, obtain accurate and complete information from airmen, and the consequences of falsification. In addition, FAA revised the privacy act statement on the 8500-8 application to include a statement that the record may be used to disclose information to other Federal agencies for verification of the accuracy or completeness of the information.

FAA had discussions on a draft matching agreement with SSA in June 2009, but a target date for completion has not been determined. FAA is holding ongoing internal discussions within the Department of Transportation to complete its review of the draft agreement. In addition, FAA has not made progress with other disability benefits providers, and reaching computer matching agreements has been a challenge—largely due to complications of sharing agency information.

When we began this audit, FAA's Office of Aerospace Medicine did not plan to implement an amnesty program to pilots who falsified their medical certificate application.¹¹ In our view, an amnesty program would provide an opportunity to quickly mitigate the safety risk posed by airmen's undisclosed and potentially disqualifying medical conditions.¹² FAA initially concluded there is no advantage in offering an amnesty program to encourage voluntarily reporting of falsifications because the proposed computer matching program between FAA and benefits providers would discover all of the pilots who have reported conflicting medical information to agencies. Further, FAA stated that an amnesty program could have a negative impact on its regulatory and enforcement activities. However, FAA has since reconsidered the utility of amnesty programs. On April 5, 2010, FAA announced a one-time, limited opportunity for airmen to reveal previously undisclosed depression and use of certain antidepressant medications without being subject to FAA enforcement action for failure to disclose this information on past medical certificate applications.¹³ This is a positive step, but we recommend that FAA move forward with finalizing and implementing computer matching

¹¹ Falsification of FAA Airman Medical Certificate Applications by Disability Recipients (CC-2007-063, July 17, 2007). The DOT Inspector General previously discussed key points for mitigating the safety risks posed by airmen who falsify their Airman Medical Certificate applications to conceal disqualifying medical conditions. OIG reports and testimony can be found on our Web page: www.oig.dot.gov.

¹² FAA previously offered a similar program in the late 1980s to identify previously undisclosed drug- or alcohol-related convictions, resulting in more than 11,000 pilots making disclosures.

¹³ To participate in this program, an airman must surrender for cancellation to the Federal Air Surgeon any current medical certificates. The airman must apply for a medical certificate between April 5, 2010 and midnight on September 30, 2010. On the application, the applicant must disclose his or her complete history of antidepressant use, the underlying condition for which the medication was prescribed, and visits to health professionals in connection with antidepressant use or the underlying condition. If an applicant falsifies any of this information on an application made on or after April 5, 2010, the FAA may take enforcement action based on that application and the previously falsified applications. 75 Fed. Reg. 17,201 (Apr. 5, 2010).

agreements to take a comprehensive approach to the undisclosed medical conditions.

CONCLUSION

The Government is responsible for securing sensitive PII collected from the public. However, FAA could not provide such assurance for the millions of airmen PII records stored in MSS. While FAA has begun to take steps to better safeguard airmen records, the current control environment is still insufficient to prevent unauthorized or inappropriate access to airmen medical information. Gaps in continuity planning and coordination with agencies providing disability benefits further compromise MSS program integrity. FAA needs to assign a high priority to fix the weaknesses identified in this report. Until then, FAA provides little assurance that sensitive information is protected from misuse, airmen holding medical certificates are fit to fly, and the medical certification program would not be disrupted in case of system failures.

RECOMMENDATIONS

We recommend that FAA's Associate Administrator for Aviation Safety, in consultation with the FAA Chief Information Officer, implement the following actions to improve the security, reliability, and accuracy of sensitive airmen medical information and tighten controls to ensure that unqualified airmen do not receive a medical certification enabling them to fly.

Secure Sensitive Airman Records:

1. Finalize implementation of MSS application security administration improvements to ensure only authorized medical staff has access to MSS, as identified by the FAA's Federal Air Surgeon in June 26, 2009, internal memorandum and report progress to the FAA Administrator.
2. Implement restrictions on AME access to inactive airman records based on a need to know.
3. Develop documentation detailing the intended controls regarding how users function within their assigned security roles, how the MSS application enforces both access control and segregation of duties, and the features of the application to assist security administration.

Deter and Detect Unauthorized Access and Invalid Airman Data:

4. Encrypt sensitive airmen PII stored in MSS as well as MSS user passwords, and develop agreements as appropriate to ensure airmen PII provided to other systems is also encrypted.

5. Implement multifactor user authentication, as required by OMB, and the Department's Secure Remote Access capability for all MSS users with remote access to sensitive PII.
6. Require and validate that all AMEs and their staff participate in the DOT security and privacy awareness training, as well as sign the DOT Rules of Behavior.
7. Implement the audit and accountability recommendations received during the previous certification and accreditation process to help identify inappropriate access to sensitive PII (abuse of access privileges) and ensure data extract/query has been erased within 90 days from its creation date.
8. Develop edit checks on the integrity of airman application data when entered into MSS.

Configure MSS Systems to Reduce the Risk of Attack:

9. Mitigate the vulnerabilities identified by OIG on MSS computers that could allow unauthorized access and potentially jeopardize confidentiality, integrity, and availability of sensitive PII.
10. Configure MSS computer systems in compliance with applicable Government standards including ensuring vendor security updates are applied, the Web site locks the user account after three unsuccessful attempts, all passwords on the MSS database are in compliance with standards, and that the application will enforce a session lock after 15-minute inactivity for all users in accordance with OMB and DOT guidance.
11. Perform and document security testing as a continual part of the MSS development process to confirm that security features remain in effect and are still functioning properly when system changes are made.

Mitigate Contingency Planning Weaknesses that Threaten Service Continuity:

12. Acquire a back-up server, finalize the Memorandum of Understanding with the selected alternate processing site, and conduct a comprehensive contingency test at the alternate site in accordance with Government standards.
13. Upgrade the database system to a version supported by the software vendor.
14. Develop back-up database administration capability in the event the primary Database Administrator is unavailable.

Detect airmen receiving disability benefits:

15. Work with SSA and other disability benefits providers to establish a target completion date for performing computer matching to identify airmen applying for, or holding, medical certificates and receiving disability benefits.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided FAA a draft of this report on March 12, 2010, and received its written comments on May 19, 2010. FAA concurred with all recommendations but recommendation 5—implementing multifactor user authentication, as required by OMB, and the Department's Secure Remote Access capability for all users with remote access to sensitive PII stored in MSS.

FAA disagrees that multifactor authentication is required to control the remote access of AMEs and their staff to MSS, even though it is required for FAA employees/contractors' access. FAA stated it performed an assessment and determined that multifactor authentication is not required for AMEs and their staff because they can only access airmen medical data that they have entered into the system. FAA further stated OMB guidance issued in 2004 requires performance of such an assessment and does not expressly require multifactor authentication for all Web based applications. FAA's position disregards OMB guidance issued later in 2006 specifically to secure remote access to sensitive information. The purpose of multifactor authentication is to ensure user authenticity (they are who they say they are), not to authorize access to the data. Furthermore, FAA did not respond to the recommendation of restricting remote access to MSS through the Department's Secure Remote Access portal. This portal checks user computers for recent security upgrades and virus protection before allowing connections to DOT's internal networks. Without going thru this security check, computers used by AMEs, if infected, could spread viruses and compromise DOT's networks. Given this significant threat, we stand by our recommendation that FAA implement multifactor user authentication and the Secure Remote Access capability for AMEs and their staff's remote access to sensitive PII.

Although FAA concurred with the remaining 14 recommendations, we have some concerns regarding its planned implementation for two of these recommendations. Specifically:

Recommendation 2. We recommended that FAA restrict access to the records of inactive airmen based on a need to know. FAA concurred and agreed to make the changes necessary to restrict access to inactive records by September 30, 2013. However, FAA's implementation schedule is protracted and will continue to put at

risk sensitive airman information beyond the time necessary for this control to be implemented. Therefore, FAA should strongly consider revising its September 30, 2013 target completion date.

Recommendation 15. We recommended that FAA work with SSA and other disability benefits providers to establish a target completion date for a computer matching program to detect airmen applying for, or holding, medical certificates while receiving disability benefits for disqualifying conditions. FAA concurred but took the position that implementation of such a program relies on other agencies' cooperation, including participation from DOT and SSA OIGs. Both OIGs participated in comparing MSS and SSA disability data during the Operation Safe Pilot investigation. This investigation targeted the most egregious cases of falsification for criminal prosecution. Criminal investigation would not be the most effective way for FAA to address the safety concerns raised by medically unfit airmen having medical certificates. Moreover, DOT OIG does not believe it would be a necessary party to a computer matching agreement. FAA is waiting to determine if SSA OIG will participate without DOT OIG. Since implementation of computer matching agreements is not entirely within its control, FAA did not provide a target completion date. FAA also indicated that should SSA OIG decline direct participation, FAA will determine, by November 2010, possible alternatives for implementing a computer matching program. While OIG believes this is a reasonable response due to the complexity of computer matching programs, FAA will need to proactively engage SSA and others to ensure progress on this recommendation and should provide information to OIG on its progress.

FAA's formal response is included in its entirety in Appendix B.

ACTIONS REQUIRED

We consider FAA's actions already taken, as well as those planned, to be responsive except for recommendations 2, 5 and 15, subject to follow-up provisions in Department of Transportation Order 8000.1C. We request that FAA give us a written response to the recommendations noted above. Specifically, within 30 days, FAA should provide its response regarding the acceleration of the target completion date for recommendation 2, and its revised position on multifactor authentication and secure remote access requirements in recommendation 5. For recommendation 15, we request that, by December 31, 2010, FAA provide its plan for completion of the computer matching program, including a target completion date, or its alternative and a target completion date.

We appreciate the courtesies and cooperation of Department of Transportation, Federal Aviation Administration's Office of Aviation Safety; CAMI Office of Aerospace Medicine; Office of Quality, Integration, and Executive Services; and Office of Information Systems Security representatives during this audit. If you

have any questions concerning this report, please call me at (202) 366-1407 or Nathan Custer, Program Director, at (202) 366-5540.

cc: Chief Information Officer, DOT
Assistant Administrator for Financial Services/CFO, FAA
Assistant Administrator for Information Services/CIO, FAA
Federal Air Surgeon, Office of Aviation Medicine, FAA
Director, Civil Aerospace Medical Institute, FAA
Martin Gertel, M-1
Anthony Williams, ABU-100

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards prescribed by the Comptroller General of the United States. As required by those standards, we obtained evidence that we believe provides a reasonable basis for our findings and conclusions based on our audit objectives. We used the following scope and methodology in conducting this review.

We conducted this audit between March 2008 and January 2010. The review included site visits to the FAA's Civil Aerospace Medical Institute (CAMI) located in Oklahoma City, Oklahoma.

To determine if airmen's personally identifiable information (PII) is properly secured from unauthorized use or access, we interviewed officials from FAA Headquarters Office of Aviation Safety; Office of Aerospace Medicine; CAMI; Office of Quality, Integration, and Executive Services; Deputy Director of Information Systems Security; and representatives from FAA's contractor. In addition, we interviewed Aviation Medical Examiners' private medical support staff at various locations, based upon users we suspect were no longer employed based on information found in a MSS user table. We obtained, reviewed and analyzed documentation related to the confidentiality, integrity, and availability of the MSS system.

In addition, we performed a vulnerability assessment of the MSS network infrastructure, servers, Web applications, databases, and data interfaces in accordance with DOT departmental Guide to Network Security as well as applicable baseline controls. 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.

To assess FAA's progress in establishing a program to identify airmen holding current medical certificates while receiving disability pay, we performed inquiries with the FAA Office of Budget—Budget Policy Division.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

<u>Name</u>	<u>Title</u>
Nathan Custer	Program Director
Ping Sun	Program Director, IT Audit Computer Laboratory
Karen Sloan	Communication Officer
Joann Adam	Project Manager
Maria Dowds	Senior Auditor
Tim Roberts	Senior Auditor
Vasily Gerasimov	Information Technology Specialist
Seth Kaufman	Associate Counsel

APPENDIX A. MEMORANDUM FROM THE FEDERAL AIR SURGEON: JUNE 26, 2009

18



Federal Aviation
Administration

Memorandum

Date: June 26, 2009
To: Rebecca C. Leng, DOT/AIGA, JA-20
From: Frederick E. Tilton, MD, Federal Air Surgeon, AAM-1
Subject: Aerospace Medical Certification Subsystem (AMCS) Security Issues

This memo is in response to an E-Mail dated June 18, 2009 that you sent to Margaret Gilligan, AVS-1, and David M. Bowen, AIO-1, and a subsequent telecon between individuals from the FAA and members of your staff that occurred on June 19, 2009. In the memo you expressed concern that certain individuals could continue to access the AMCS system when they no longer had a legal authorization to do so. We share your concerns for the security of our systems, and we are taking these actions to correct the deficiency:

NEAR TERM – Not later than September 30, 2009

As of June 24, 2009, the following action memo pops into view every time an individual logs on to the AMCS website or the FAA.GOV AMCS support webpage.

"To ensure continued security and integrity of your aviator's medical certification information on the FAA AMCS web based system, it is critical that only current authorized users from your office have valid AMCS accounts. It is your responsibility to notify the AMCS Online Support help desk at (405) 954-3238 if staff changes have occurred for individuals with AMCS privileges and their employment status no longer requires AMCS access."

Not later than July 31, 2009, an electronic query will be transmitted across AMCS that will be used to identify any aviation medical examiner (AME) or staff member who has not accessed the AMCS system within the previous 90 days. The information will be reviewed and analyzed by aerospace medicine (AAM) management to ascertain those AMCS accounts that should be

APPENDIX A. MEMORANDUM FROM THE FEDERAL AIR SURGEON: JUNE 26, 2009

19

disabled. AAM management will then notify the IT help desk representative to disable the identified accounts. This process will be repeated quarterly.

Not later than August 31, 2009, a letter will be sent to each AME that requires him or her to promptly report any change in staff member status to the regional flight surgeon, the AMCS online support help desk, the manager of the aerospace medical certification division AAM-300, and the manager of the aerospace medical education division AAM-400. This letter will include the currently approved users for the office and emphasize that FAA security requires that AMCS usernames and passwords must not be shared with anyone. The letter will include a warning that the FAA will take an adverse action against an AME's designation if he or she should fail to comply with this requirement.

MID TERM – Not later than December 31, 2009

Train the AAM regional program analysts who perform surveillance visits to AME's offices to include an assessment of AMCS use by the AME and his or her staff.

Develop a process that automatically sends an email message to each AME on a regular basis requiring him or her to verify that each staff member who is using AMCS is authorized to do so. Non-response from the AME within 30 days will result in account disablement for that AME and associated staff members.

Provide the results of the electronic query noted above to the AAM regional flight surgeons for enhanced oversight of AME activity. In addition, the regional flight surgeons will conduct random checks to help assure compliance.

LONG TERM – Not later than September 30, 2010

Revise the AME Order to add "AME failure to immediately notify the FAA about changes in the status of AME staff who are AMCS users" to the list of reasons that could result in termination of an AME's designation.

As part of the tri-annual AME re-designation process, AMEs will be required to validate the current status of their staff members who have access to AMCS.

When we issue AMCS usernames and passwords to AMEs and their staffs we will require them to sign a statement indicating that they agree to stop accessing AMCS whenever they no longer have the legal justification to use this system.

**APPENDIX A. MEMORANDUM FROM THE FEDERAL AIR
SURGEON: JUNE 26, 2009**

20

Develop a software modification to the AMCS logon procedure that will automatically require each AME to validate the authorized users in his or her office each quarter.

In closing, as you know, we are legally required to monitor and assess the security controls of our systems and to take appropriate actions to enhance and improve them as necessary.



Federal Aviation Administration

Memorandum

Date: MAY 19 2010

To: Rebecca C. Leng, Assistant Inspector General for Financial and Information Technology Audits

From: Ramesh K. Punwani, Assistant Administrator for Financial Services/CFO

Prepared by: Anthony Williams, x79000 

Subject: OIG Draft Report: Information Security and Privacy Controls over the Airmen Medical Support Systems Federal Aviation Administration

The Federal Aviation Administration (FAA) is committed to ensuring the security of our information systems and the privacy of personal information in our systems. Over the past year, the FAA has taken steps to tighten access requirements and controls for the Airmen Medical Support System (MSS), increase the use of encryption, and correct security vulnerabilities identified in the report. As part of a complete database upgrade in October 2009, the FAA also deployed backup servers, and added processing capability at an alternate location. The FAA will complete additional work through next year that will further strengthen system security and protection of personally identifiable information (PII).

The FAA plans to establish a Federal database matching program to identify pilots who have falsified their FAA Application for Airman Medical Certificate (FAA Form 8500-8). To improve the safety of the National Airspace System, the FAA plans to identify pilots who receive disability benefits from the Social Security Administration (SSA), Veterans Administration (VA) or Department of Labor (DOL). The FAA recognizes that pilots may meet disability standards at SSA, VA or DOL yet still satisfy FAA medical standards, or be eligible for a special issuance medical certificate. As a result, the FAA will need to carefully review any match between data bases and review the medical information in those data bases to ensure that pilots have fully and accurately reported their medical histories to the FAA. The FAA will initiate appropriate enforcement actions in cases where pilots have falsified their Application for an Airman Medical Certificate.

Attachment

Appendix B. Agency Comments

OIG Recommendations and FAA Responses

OIG Recommendation 1. Finalize implementation of MSS application security administration improvements to ensure only authorized medical staff has access to MSS, as identified by the FAA's Federal Air Surgeon in June 26, 2009, internal memorandum and report progress to the FAA Administrator.

FAA Response: Concur. The FAA implemented security measures that have already improved MSS application security administration. Work on additional measures is underway with completion planned for the end of Fiscal Year (FY) 2010. The following is a listing of actions completed and underway.

COMPLETED ACTIONS:

User Warning Message – The following warning message, which is displayed when any user logs in to the Airmen Medical Certification System (AMCS), was implemented in June 2009:

“To ensure continued security and integrity of your aviator’s medical certification information on the FAA AMCS web based system, it is critical that only current authorized users from your office have valid AMCS accounts. It is your responsibility to notify the AMCS Online Support help desk at (405)954-3238 if staff changes have occurred for individuals with AMCS privileges and their employment status no longer requires AMCS access.”

User Account Inactivity Report – The FAA developed an automated query to help identify users that may no longer require access to the system. The query generates quarterly reports of MSS accounts which have not accessed the system within the last 90 days. This report can be run at any time and for any duration (i.e. 30, 60, 90 days, etc.) of inactivity.

User Requirement Notification – A letter notifying each AME of their responsibility to report staff changes was mailed to each AME on September 21, 2009.

Train FAA Designee Surveillance Staff – The FAA developed and conducted training for FAA employees who are assigned designee oversight and quality assurance responsibilities. This AME surveillance training was held in October 2009.

AME Verification – In December 2009 the FAA implemented an automated process for sending E-Mail messages to AMEs on a regular basis requiring verification for each of their staff members authorized to access AMCS.

APPENDIX B. AGENCY COMMENTS

23

Electronic Query Results Reporting – FAA Regional Flight Surgeons received their first reports from the verification queries in December 2009. This reporting will improve designee oversight and will continue until the final MSS software modification is functional.

Tri-Annual AME Staff Access Revalidation – Beginning in October 2009, AMEs are required to review all members of their staff who have MSS access and confirm that they are still employed by the AME and still require access to MSS.

Signed Verification of Need for Access to MSS – FAA requires AMEs and their staffs to complete and sign an account request form to obtain their user names and passwords. The form they sign includes a statement that they agree to notify the FAA and stop accessing MSS when they no longer have a legal justification to do so. Specifically the statement reads:

"I agree to promptly notify the Aeromedical Certification Division/AAM-300 of any changes in the status of the requestor's employment or in the event that the requestor (AME, Staff, or FAA Employee/Contractor) no longer has the need-to-know requirements concerning the above computer system."

ACTIONS UNDERWAY – The following actions are underway and are intended for completion by the end of FY 2010:

Revise FAA AME Order – A revision to FAA Order 8520.2, incorporates a new provision as a cause to terminate an AME designation. Under the new provision, an AME may be terminated for failure to notify the FAA of staff changes for those with access to AMCS. The revisions incorporated in this change to the order focus on FAA designee management standards. The order is ready for internal FAA coordination and the projected publication date is August 2010.

Improved User Authentication – The FAA is developing MSS software modifications to require AMEs to validate authorized users quarterly. Portions of the software modifications have been completed and deployed, including the web page, which AMEs will use to validate staff members. This web page was available in December 2009 for AMEs to begin validating staff with continuing need to access the MSS. This same web page will be used by AMEs when they are required, as part of the AMCS logon process, to validate their staff personnel each quarter. Full implementation of the AMCS logon validation procedure is slated to be completed and deployed by August 31, 2010.

OIG Recommendation 2. Implement restrictions on AME access to inactive airman medical records based on a need to know.

FAA Response: Concur.

In addition to all the restrictions currently in the MSS system, the FAA will develop the necessary MSS software changes for designating airmen medical records as inactive and

APPENDIX B. AGENCY COMMENTS

24

restricting access to inactive records for aerospace medicine research purposes only. While the FAA concurs with the recommendation, a number of interim measures must be addressed to achieve implementation. First, the FAA needs to begin with a business process to define an "inactive airman" from the perspective of medical certification. While deceased airmen are discussed in the report, the FAA is not typically informed when an airmen dies through non-aviation related events. AVS could base the definition on the valid period for a third class medical certificate with a grace period added to minimize inefficient shuffling of airmen records between an active and inactive status. Determining the length of the grace period could be supported by queries of historical examination records. After the FAA determines a standard for inactivity, it will need to develop business processes and application modifications to restrict AME and employee access to records of inactive airmen. The FAA will also need to concurrently develop business processes that return records to an active status, if appropriate, without an undue burden on the airmen or designees. The target date for completing the actions relating to this recommendation is no later than September 30, 2013. As discussed above, this will require interim actions, which will be completed as follows:

- Complete analysis of MSS airmen data – September 30, 2010
- Complete development of active/inactive airmen business rules – December 31, 2010
- Complete analysis of required MSS modifications – May 31, 2011
- Complete plan for MSS modifications, cost estimates and schedule – September 30, 2011
- Task MSS modifications to contractor – December 31, 2011
- Completion of all MSS modifications – September 30, 2013

OIG Recommendation 3. Develop documentation detailing the intended controls regarding how users function within their assigned security roles, how the MSS application enforces both access control and segregation of duties, and the features of the application to assist security administration.

FAA Response: Concur.

During the fiscal year (FY) 2009 annual security assessment of the MSS applications, AVS developed documentation that details user functions within their assigned security roles. The activities necessary to complete the remaining aspects of this recommendation must be completed in two sequential steps. Actions to complete documentation describing how the MSS applications enforce access control and separation of duties is included in the departmental FISMA reporting system, with a due date of September 30, 2010. Once the access control and separation of duties documentation is complete¹, the FAA can begin developing documentation for security administrators that describes the features of the application, which is being tracked with a due date of September 30, 2011.

¹ The FAA assumes "segregation of duties" is synonymous with "separation of duties" as defined in control AC-5, Separation of Duties, in NIST Special Publication 800-53.

APPENDIX B. AGENCY COMMENTS

25

OIG Recommendation 4. Encrypt sensitive airmen PII stored in MSS as well as MSS user passwords, and develop agreements as appropriate to ensure airmen PII provided to other systems is encrypted too.

FAA Response: Concur.

The FAA began encrypting the tables containing user passwords and airmen PII as part of the database upgrade, which was completed on October 13, 2009. Encryption to protect the transfer of records to the Aviation Registry will be implemented in accordance with the AVS Privacy Implementation Plan. As part of the 2010 security assessment of the Aviation Registry and MSS systems, the FAA will create Plan of Action and Milestones (POA&Ms) to reflect the OIG recommendation to encrypt the data transfer between MSS and the Aviation Registry. An MOU for data transfer between MSS and the Aviation Registry is not necessary because these two systems are under the management control of the Associate Administrator for Aviation Safety and FAA Order 1370.82A, *Information Systems Security Program*, specifically states that an agreement is not required.

The security controls to protect airmen PII provided for computer record matching with the National Driver Registry (NDR) are in place, including encryption. AVS is developing a memorandum of understanding with the Office of Security and Hazardous Materials (ASH) to formalize the information exchange and security requirements. The target date for completing the ASH MOU and data encryption between MSS and the Aviation Registry is September 30, 2011.

OIG Recommendation 5. Implement multifactor user authentication, as required by OMB and the Department's Secure Remote Access capability for all MSS users with remote access to sensitive PII.

FAA Response: Non-Concur.

The MSS consists of multiple software components. The FAA updated the Information System Security Plan (ISSP) and E-Authentication Analysis in 2009 to provide a clear rationale for the differing access levels for the different MSS component applications. Remote FAA users who can fully access all MSS data and applications must use multifactor authentication. AMEs, their staffs and airmen have significantly restricted access to MSS data and applications. AMEs and their staffs may only access one web based application, AMCS, and can only access airmen medical data that they have entered into the system. Airmen only have access to MedXpress which allows them to submit their personal identifying and medical information for their next examination. Because of the limited system access, the FAA determined that AMEs, AME staff, and airmen only require user ID and password authentication (NIST SP800-63 Level 2).

OMB does not require multifactor authentication for all web based applications. OMB Memorandum 04-04 directed agencies to perform an assessment of the authentication requirements for applications, such as AMCS and MedXpress. The results of an assessment following OMB guidance can range from as little as user ID alone for a Level

APPENDIX B. AGENCY COMMENTS

26

1 application up to multifactor authentication (including hard token) for Level 4 applications. FAA documented the AMCS and MedXpress assessments in both 2008 and 2009 E-Authentication Analyses. No further action is planned on this recommendation.

OIG Recommendation 6. Require and validate that all AMEs and their staff participate in the DOT security and privacy awareness training, as well as sign the DOT Rules of Behavior.

FAA Response: Concur.

FAA agrees to provide AMEs and their staff with appropriate security and privacy awareness training. Since AMEs and their staff have access to a single FAA application, and access within that application is already very limited, their training will be more focused and specialized than the DOT employee and contractor training which is intended for users with network access to multiple DOT applications. In developing and delivering appropriate training, the FAA must carefully balance the benefits of security awareness training with the burdens it places on AMEs, who assist the FAA in performing a critical aviation safety function, but are not compensated by the government.

Additionally, as health care providers, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the U.S. Department of Health and Human Services (HHS) implementing regulations in 45 CFR Parts 160 and 164 apply to AMEs and their staffs. 45 CFR Part 164.308(a)(5)(i) addresses Security Awareness and Training and requires the implementation of a security awareness and training program. HHS enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information and the HIPAA Security Rule, which sets national standards for the security of electronic protected health information.

Recognizing the benefits of security awareness training, the FAA will develop and incorporate appropriate security and privacy awareness training into both basic and recurrent AME training. The FAA will also reinforce security awareness for AMEs and their staff through recurring articles in the Federal Air Surgeon's Medical Bulletin that is published quarterly and distributed to all AMEs. Although the current *AMCS Account Request* form includes many items associated with "Rules of Behavior", the FAA will review its Rules of System Use (RoSU) and update the form as required. In addition, the FAA will add security messages to the AMCS "splash" screen, requiring the user to acknowledge the message before accessing the application. The target date for completing all actions associated with this recommendation is September 30, 2011. Interim milestones include:

- Complete review of RoSU – September 30, 2010
- Update RoSU – December 31, 2010
- New AMCS security/privacy messages deployed to the AMCS "splash screen" - March 31, 2011

APPENDIX B. AGENCY COMMENTS

27

- Deploy new initial and recurrent AME security and privacy training – September 30, 2011

OIG Recommendation 7. Implement the audit and accountability recommendations received during the previous certification and accreditation process to help identify inappropriate access to sensitive PII (abuse of access privileges) and ensure data extract/query has been erased within 90 days from its creation date.

FAA Response: Concur.

The remediation item to implement an audit process and capability into MSS is entered in the departmental FISMA reporting system with a due date of September 30, 2011.

OIG Recommendation 8. Develop edit checks on the integrity of airman application data when entered into MSS.

FAA Response: Concur.

The functional requirements document for MSS includes edit check capability to ensure the integrity of airman application data. OIG testing of MSS indicated that required edit checking of airmen data was not taking place within the application. The FAA will test the edit checking capability within MSS and ensure that it is working. Milestones for this OIG recommendation are as follows:

- Complete validation testing of the MSS application suite – September 30, 2010.
- Implement corrective measures within MSS where the validation process identifies inconsistencies with the functional requirements document – September 30, 2011.

OIG Recommendation 9. Mitigate the vulnerabilities identified by OIG on MSS computers that could allow unauthorized access and potentially jeopardize confidentiality, integrity, and availability of sensitive PII.

FAA Response: Concur.

FAA reviewed and corrected findings provided to the Program Manager for the MSS applications. Following the correction of vulnerabilities identified in the scan of MedXPress, the Program Manager reviewed the other MSS component applications based on these findings. The hosting infrastructure for the MSS application has been completely replaced. The servers are regularly monitored for missing security updates and other vulnerabilities and appropriate action has been taken in each instance. This action was completed October 13, 2009.

OIG Recommendation 10. Configure MSS computer systems in compliance with applicable Government standards including ensuring vendor security updates are applied, the Web site locks the user account after 3 unsuccessful attempts, all passwords on the MSS database are in compliance with standards, and that the application will enforce a

APPENDIX B. AGENCY COMMENTS

28

session lock after 15-minute inactivity for all users in accordance with OMB and DOT guidance.

FAA Response: Concur.

The FAA will ensure that MSS computer systems are configured in compliance with applicable standards by September 30, 2011. AVS developed several Baseline Security Configuration Standards (BSCS) for commercial products, including common databases. An AVS BSCS was used as a foundation for the security configuration during the database upgrade. Recent DOT policy changes require configuration and assessment using a NIST or DOT approved checklist. AVS will review available database checklists and implement an appropriate checklist for compatibility with enterprise infrastructure and business requirements. To ensure the MSS servers maintain their approved security configuration, AVS will continue its vulnerability scanning program which regularly scans the server infrastructure that hosts the MSS applications and addresses vulnerabilities.

The MSS web-enabled applications were modified on August 14, 2008 to lock user accounts after three unsuccessful attempts. This modification also requires user passwords to comply with FAA Order 1370.92, *Password and PIN Management*.

As noted in our response to OIG Recommendation 6 above, AMEs and their staffs are required to comply with HIPAA and the HHS implementing rules. The FAA will specify a specific time out value for AME desktops in their AMCS access agreements. While NIST recommends a 15 minute value, the FAA will discuss this specific value with the AME community and establish a value that complies with OMB, DOT and HHS requirements for information systems security. The target date for establishment and implementation of all time out standards is September 30, 2011.

OIG Recommendation 11. Perform and document security testing as a continual part of the MSS development process to confirm that security features remain in effect and are still functioning properly when system changes are made.

FAA Response: Concur.

The remediation item to document security testing as a continual part of the MSS development process is entered in the departmental FISMA reporting system with a due date of September 30, 2010.

OIG Recommendation 12. Acquire a back-up server, finalize the Memorandum of Understanding with the selected alternate processing site, and conduct a comprehensive contingency test at the alternate site in accordance with Government standards.

FAA Response: Concur.

APPENDIX B. AGENCY COMMENTS

29

These actions were completed in October 2009. FAA brought the backup server online as part of the database upgrade in October 2009. This provides redundant servers at the primary processing site. The Application Hosting Proposal was finalized on August 19, 2009. This MOU documents the facility requirements for a data center in the event of a disaster at the primary processing site. The MSS application was recovered at the back up site on September 14, 2009 during a comprehensive contingency test.

OIG Recommendation 13. Upgrade the MSS database system to a version supported by the software vendor.

FAA Response: Concur.

FAA completed the MSS database upgrade on October 13, 2009.

OIG Recommendation 14. Develop back-up database administration capability in the event the primary Database Administrator is unavailable.

FAA Response: Concur.

FAA completed this recommendation in April 2009 through the addition of support staff.

OIG Recommendation 15. Work with SSA and other disability benefits providers to establish a target completion date for performing computer matching to identify airmen applying for, or holding, medical certificates and receiving disability benefits.

FAA Response: Concur.

The FAA has made significant progress in response to the House Aviation Subcommittee's request that the FAA establish a matching program that would enable FAA to detect airmen receiving disability benefits, compare medical records to ensure medical information was appropriately disclosed, and determine whether enforcement action is warranted.

FAA has completed the necessary legal steps that would allow the agency to share medical information with other Federal agencies. Through publication in the Federal Register, the FAA notified the public that it had revised the system of records notice that applies to airman medical records to include one that expressly authorizes disclosure of airman medical information to other Federal agencies for verification of the accuracy and completeness of the applications. In addition, the Application for Airman Medical Certificate, FAA Form 8500-8, was revised to provide similar information to each airman medical certificate applicant.

The FAA also completed measures to obtain disability-related information directly from applicants for an airman medical certificate. The FAA revised its paper and web-based versions of its Application for Medical Certificate, FAA Form 8500-8, to require airmen to address whether they currently receive, or have ever received, medical disability

APPENDIX B. AGENCY COMMENTS

30

benefits. In addition, the FAA is providing written and oral instruction to its cadre of approximately 4,000 AMEs by way of the Federal Air Surgeon's Medical Bulletin and at AME seminars describing their responsibility to seek disability-related information from airmen.

While FAA has put into place these necessary building blocks that are within its authority, it has not yet succeeded in gaining the cooperation of the other entities necessary to make the process work. FAA's limited data match testing during "Operation Safe Pilot," was made possible through the participation of the DOT-OIG and the Social Security Administration OIG (SSA-OIG). FAA's efforts to build upon Operation Safe Pilot relies upon the continued cooperation of both OIGs, and to date, DOT-OIG has declined to participate. Recently, the DOT-OIG informed the FAA that it would not participate in a computer matching program as proposed by the SSA-OIG. The FAA notified the SSA-OIG of the DOT-OIG's decision not to participate and requested the SSA-OIG to consider the feasibility of proceeding without DOT-OIG involvement. The FAA is awaiting SSA-OIG's response to this request. If SSA-OIG declines direct participation with FAA, then FAA will determine by November 2010 whether there may be alternative avenues to pursue the data match program.

Based upon the FAA's limited experience and involvement with DOT OIG and SSA OIG pilot matching program "Operation Safe Pilot", it is clear that FAA will require additional personnel and funding to carry out nation-wide, multi-departmental matching program. Operation Safe Pilot only focused on the Northern and Eastern Districts of California, and it generated a significant work load for the FAA Western-Pacific Aerospace Medicine Division. The FAA needs physicians, program analysts, attorneys and paralegal specialists to implement and carry out a national program to investigate alleged instances of falsification, prepare appropriate documentation in support thereof, and carry out enforcement actions consistent with the Federal Aviation Regulations.

The FAA will seek additional resources in the President's FY 2012 and/or FY 2013 budget request to implement and carry out this program. If the other Federal entities are willing to participate, the FAA will be prepared to begin the program in FY 2012.