Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued August 18, 2017

Massachusetts Department of Transportation Aeronautics Division—Information Technology

For the period July 1, 2014 through December 31, 2015

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

August 18, 2017

Mr. Jeffrey DeCarlo, Administrator
Massachusetts Department of Transportation, Aeronautics Division
Logan Office Center
One Harborside Drive, Suite 205N
East Boston, MA 02128-2909

Dear Mr. DeCarlo:

I am pleased to provide this audit of the Massachusetts Department of Transportation's Aeronautics Division. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2014 through December 31, 2015. My audit staff discussed the contents of this report with management of the agency, whose comments are reflected in this report.

I would also like to express my appreciation to the Aeronautics Division for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Stephanie Pollack, Secretary, Massachusetts Department of Transportation

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Air-PORT	Airport Information Resource Portal
CMR	Code of Massachusetts Regulations
COBIT	Control Objectives for Information and Related Technology
FAA	Federal Aviation Administration
ISACA	Information Systems Audit and Control Association
ISP	information security program
IT	information technology
ITGC	information technology general control
MassDOT	Massachusetts Department of Transportation
MMARS	Massachusetts Management Accounting and Reporting System

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted an audit to review and evaluate controls over selected information technology (IT) operations and activities at the Massachusetts Department of Transportation (MassDOT) Aeronautics Division for the period July 1, 2014 through December 31, 2015. We extended our audit period through September 2016 to accommodate our audit test of IT governance and October 2016 for aircraft registration. We performed our testing for logical access security as of August 2016.

In this audit, we reviewed certain IT general controls over the Aeronautics Division's Airport Information Resource Portal (Air-PORT) application that were related to IT project management, IT governance, and logical access security. We also followed up on the issues identified in our previous audit of the Aeronautics Division (No. 2008-0044-4T) regarding the implementation of controls related to aircraft registrations and the revenue generated.

Our audit of the Aeronautics Division identified an issue that has been omitted from this report in accordance with Exemption (n) of the Commonwealth's public-records law (Section 7[26] of Chapter 4 of the General Laws), which allows for the withholding of certain records, including security measures or any other records related to cybersecurity or other infrastructure, if their disclosure is likely to jeopardize public safety or cybersecurity.

In accordance with Sections 7.39–7.43 of the Government Accountability Office's Government Auditing Standards, as well as the policies of the Office of the State Auditor, for reporting confidential and sensitive information, we have given a separate, full report to the Aeronautics Division, which will be responsible for acting on our recommendations.

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1a **Page 8**	Ineffective IT project management resulted in deficiencies in Air-PORT.
Finding 1b **Page 9**	The Aeronautics Division did not periodically review its Web-hosting service provider's security measures.
Finding 1c **Page 10**	The Aeronautics Division did not grant user access to Air-PORT based on business need.

Finding 1d **Page 11**	The Aeronautics Division still had not documented and tested a business-continuity plan.
Finding 1e **Page 12**	Aeronautics Division employees did not receive security-awareness training.
Recommendations **Page 13**	1. The Aeronautics Division should ensure that all future IT projects are staffed with personnel with expertise in IT project management. Further, IT projects should have detailed business and technical application requirements. 2. MassDOT should amend its Software Development & Maintenance Policy to require the involvement of MassDOT IT for Aeronautics Division–managed IT projects that MassDOT IT staff has adequate expertise to administer. 3. The Aeronautics Division should establish business requirements and a process to periodically review the effectiveness of its third-party service providers' security measures. The process should clearly define who is responsible for performing this review and should be defined in policies and procedures. 4. The Aeronautics Division should immediately remove all external consultants' accounts and test accounts from Air-PORT. MassDOT should establish a process to review the Air-PORT user accounts to ensure that access is based on business need. This process should clearly define the roles and responsibilities for performing the review. 5. The Aeronautics Division, in conjunction with MassDOT IT, should develop, document, and test a business-continuity plan in accordance with the Enterprise Business Continuity for IT Management Policy. 6. The Aeronautics Division should ensure that all employees receive security-awareness training upon hire and annually.
Finding 2a **Page 15**	The Aeronautics Division did not provide adequate oversight of airport managers' required semiannual reports.
Finding 2b **Page 16**	The Aeronautics Division lacked adequate monitoring and evaluation controls over the accuracy and completeness of its aircraft registration database.
Recommendations **Page 17**	1. The Aeronautics Division should establish formal policies and procedures to ensure that airport managers' reports are received twice a year. At a minimum, such policies and procedures should establish a standard report format, require following up with airports that do not submit the required reports, and establish penalties for noncompliance. 2. The Aeronautics Division should establish a process of periodic reporting to management that would identify aircraft without a registration status or with data-entry errors; reconcile the total amount of aircraft registration fees recorded as collected in the state's Massachusetts Management Accounting and Reporting System and the amount recorded in Air-PORT; and ensure that all aircraft listed in airport managers' reports are in Air-PORT.

OVERVIEW OF AUDITED ENTITY

The Massachusetts Department of Transportation (MassDOT) Aeronautics Division, formerly known as the Massachusetts Aeronautics Commission, was authorized by Chapter 90 of the Massachusetts General Laws. The Aeronautics Division has jurisdiction over 36 of the Commonwealth's 39 public-use airports. It does not have jurisdiction over activities at Logan International Airport, Worcester Airport, or Hanscom Field, which are owned and operated by the Massachusetts Port Authority.

According the Aeronautics Division's website, its mission is "promoting aviation across the Commonwealth while establishing an efficient, integrated airport system that is focused on airport safety, customer service, economic development, and environmental stewardship." The Aeronautics Division's mission-critical and essential application system is the Airport Information Resource Portal (Air-PORT), which was established to replace the division's Airport Information Management System in 2013. According to Air-PORT's user manual, Air-PORT is a "web-based application . . . [that] facilitates the management of facility information, projects and grants, and other activity data across the MassDOT system, and . . . supports cloud data storage and retrieval." The intended users of the Air-PORT application include Aeronautics Division employees, airport managers, airport consultants, and airport personnel.

MassDOT provides the Aeronautics Division with overarching governance for internal control planning, program support, and overall funding. The Aeronautics Division's processing capabilities and business-continuity planning are supported by MassDOT's Information Technology Department.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted an audit of certain activities of the Massachusetts Department of Transportation (MassDOT) Aeronautics Division for the period July 1, 2014 through December 31, 2015. We extended our audit period through September 2016 to accommodate our audit test of information technology (IT) governance and October 2016 for aircraft registration. We performed our testing for logical access security as of August 2016.

In this audit, we reviewed certain IT general controls (ITGCs) over the Aeronautics Division's Airport Information Resource Portal (Air-PORT) application that were related to IT project management, IT governance, and logical access security. ITGCs are a subset of internal controls that are applied to every IT system that an organization relies on and to the IT staff that administers those systems. ITGCs assure management and stakeholders of the reliability of data and information systems. The objective of ITGCs is to ensure the confidentiality, integrity, and availability of systems, programs, data files, and computer operations in an organization.

We also followed up on the issues identified in our previous audit of the Aeronautics Division (No. 2008-0044-4T) regarding the implementation of controls related to aircraft registrations and the revenue generated.

We conducted this audit 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.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and where each objective is discussed in the audit findings.

Objective	Conclusion
1. Has the Aeronautics Division established adequate ITGCs to support its mission-critical and essential application system over the following areas?	

Objective	Conclusion
a. IT project management, including contracts and service-level agreements	**No; see Finding 1a**
b. logical access security, including user account management	**No; see Finding 1c**
c. IT governance, including IT policies and procedures, new employee acknowledgment forms, and employee security-awareness training	**No; see Finding 1e**
d. business continuity, including a documented and tested business-continuity plan that includes a continuity-of-operations plan and a disaster-recovery plan to provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems and applications be rendered inoperable or inaccessible	**No; see Findings 1b and 1d**
2. Has the Aeronautics Division implemented adequate controls regarding the registration process for aircraft under its jurisdiction and the revenue the division generated for calendar year 2015?	**No; see Findings 2a and 2b**

We conducted this performance audit using criteria from MassDOT's information security program (ISP), which dictates how the Aeronautics Division keeps data secure and reduces the risk of unauthorized disclosure. If MassDOT's ISP was deficient in a certain area, we relied on industry standards established by the Information Systems Audit and Control Association (ISACA) in Control Objectives for Information and Related Technology (COBIT) 4.1 and by the Massachusetts Office of Information Technology. Although the Aeronautics Division is not required to follow COBIT industry standards, we believe they represent IT industry best practices for ITGCs. For example, the purpose of COBIT is to provide management and business process owners with an IT governance model that helps deliver value from IT and understand and manage the risks associated with IT. According to ISACA's website,

> *COBIT helps bridge the gaps amongst business requirements, control needs and technical issues. It is a control model to meet the needs of IT governance and ensure the integrity of information and information systems.*

We gained an understanding of the internal controls we deemed significant to our audit objectives through interviews and observations. To achieve our objectives, we performed the following audit procedures:

- We assessed the Aeronautics Division's ITGCs over Air-PORT. Specifically, we performed the following procedures:

- We interviewed Aeronautics Division and MassDOT IT staff members to obtain an understanding of the Air-PORT project-management approach used to replace the division's Airport Information Management System.

- We obtained and reviewed the Aeronautics Division's request for responses[1] to replace its Airport Information Management System to determine the implementation period and budget and whether the Aeronautics Division evaluated third-party services objectively.

- We obtained and inspected contracts with third-party vendors for Air-PORT to determine whether contracts were in place throughout the project and whether the scope of work to be performed, including detailed design and technical application requirements, was approved by both parties.

- We asked management whether periodic reviews of access were performed on Air-PORT. We reviewed access for all 33 users of the application to determine whether access was limited to individuals with a business need and whether user accounts were uniquely identifiable.

- We performed a walkthrough of user permissions within all access levels of Air-PORT to determine whether segregation of duties was in place. We did not test all functionalities within the system.

- We reviewed various Aeronautics Division internal control documents (including its ISP, organization charts, mission statement, internal control plan, information security handbook, and Password and Acceptable Use Policy) and interviewed the director of Finance and Administration, MassDOT's IT director, and other staff members to obtain an understanding of the Aeronautics Division's IT governance.

- We asked management whether all employees had security-awareness training that properly educates users on how to protect the confidentiality and integrity of MassDOT's systems and information by ensuring that they have a solid understanding of MassDOT's security directives, procedures, and best practices.

- We reviewed signed Acceptable Use of Information Technology Resources forms for all new employees to determine whether employees acknowledged their responsibility as employees of MassDOT for security, data protection, and data confidentiality before gaining access to MassDOT information.

- We interviewed Aeronautics Division and MassDOT IT management to determine whether a written business-continuity plan, a disaster-recovery plan, and a continuity-of-operations plan were in place; and, if so, whether the plans were adequately tested.

- We interviewed Aeronautics Division and MassDOT IT management to determine whether the security measures for their Web-hosting service provider were periodically assessed for effectiveness.

1. A request for responses is a document that state government agencies draft during competitive procurement.

- We assessed the Aeronautics Division's aircraft registration process and revenue generated for calendar year 2015. Specifically, we performed the following procedures:

  - We requested all 36 airport managers' reports that had been sent to the Aeronautics Division for calendar year 2015. We examined the reports to determine whether they could be used to effectively perform reconciliations between airport managers' reports and Air-PORT.

  - We asked Aeronautics Division management whether aircraft owner registration reports were in place to provide Aeronautics Division management with a formal report of the total population of aircraft owner fees that were due or had been paid.

  - We asked Aeronautics Division management and other staff members if they had inspected aircraft to determine whether flying condition and state of repair could help determine whether airplanes need to be registered.

  - We examined aircraft registration credits from our audit period and judgmentally selected a sample of 3 out of a population of 10 records to verify that credits were supported by adequate documentation and approval. Because our sampling was nonstatistical, we did not project the results of our audit tests to the total populations in the areas we reviewed.

  - We examined aircraft registration revenue with duplicate check numbers from our audit period and judgmentally selected a sample of 65 out of a population of 672 duplicate check number records to verify that records were supported by adequate documentation and the proper revenue amounts were collected and recorded in the Massachusetts Management Accounting and Reporting System (MMARS). Because our sampling was nonstatistical, we did not project the results of our audit tests to the total populations in the areas we reviewed.

- We assessed the reliability of the Aeronautics Division's data for the Air-PORT user-account list, the human-resource system, the Air-PORT aircraft registration database for 2015, the MMARS database and the Federal Aviation Administration database by (1) performing electronic testing of required data elements, (2) reviewing existing information about the data and the system that produced them, (3) interviewing agency officials who were knowledgeable about the data, and (4) observing the data extract. In addition, we relied on the results of our data-reliability assessment of MMARS dated April 8, 2014, which tested general IT controls for system design and effectiveness, including: accessibility of programs and data, system change management, and policies and procedures for applications, configurations, jobs, and infrastructure. We determined that the data used were sufficiently reliable for the purposes of this report.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Aeronautics Division had deficiencies in information technology project management and general controls over logical access, business-continuity planning, and security-awareness training.

The Aeronautics Division had deficiencies in information technology (IT) general controls over its Airport Information Resource Portal (Air-PORT) application system[2] and its business operations. Specifically, the division had inadequate controls in IT project management, logical access, business-continuity planning, and security-awareness training. The deficiencies could have compromised the integrity, availability, and confidentiality of the Aeronautics Division's information. Further, Aeronautics Division and Massachusetts Department of Transportation (MassDOT) IT management told us that Air-PORT, as developed, does not fully meet the Aeronautics Division's business needs and may need to be replaced. This would result in a significant waste of staff resources and of the more than $600,000 that was spent in developing Air-PORT.

a. Ineffective IT project management resulted in deficiencies in Air-PORT.

Between fiscal years 2012 and 2015, the Aeronautics Division hired a contractor, CDM Smith, to develop and implement Air-PORT to replace its Airport Information Management System at a total cost of $603,958. However, the Aeronautics Division did not effectively administer the development of Air-PORT. As a result, because Air-PORT was not meeting business needs, the Aeronautics Division and MassDOT IT determined that the application, as designed, was deficient and might need to be replaced with a more efficient and effective solution. This would result in a significant waste of money and other staff resources.

Specifically, the Aeronautics Division established high-level business requirements for general system information, project planning, project management, budget and finance, airport inspections, aircraft registrations, accident investigations, airspace reviews, and contact lists. However, it did not provide detailed design and technical application requirements defining how the system should function. Further, the new Aeronautics Division administrator, who was appointed on August 31, 2015, signed a $50,000 contract in November 2015 to, among other things, fix Air-PORT defects that

2. This system contains owner and aircraft information such as aircraft number, purchase date, weight, make, model, registration fee, and payment information.

agency staff members had identified. However, after the contract was signed, the division identified additional critical bugs and necessary future enhancements that were not covered by the contract.

Authoritative Guidance

Section AI.2 of Control Objectives for Information and Related Technology (COBIT) 4.1 requires that, when organizations develop an application system, they do the following:

> *Prepare detailed design and technical software application requirements. Define the criteria for acceptance of the requirements. . . .*
>
> *Implement business controls, where appropriate, into automated application controls such that processing [of data] is accurate, complete, timely, authorised and auditable. . . .*
>
> *Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties.*

Reasons for Noncompliance

According to Aeronautics Division officials, the staff members involved in the Air-PORT project lacked expertise in IT project management. In addition, MassDOT's 2016 Software Development & Maintenance Policy does not require MassDOT IT, which may have the expertise necessary to administer this project effectively, to be involved in projects managed by the Aeronautics Division.

b. The Aeronautics Division did not periodically review its Web-hosting service provider's security measures.

The Aeronautics Division did not establish a process to ensure that security measures provided by its third-party Web-hosting service provider for Air-PORT were sufficient. This process would have included defining the roles and responsibilities for reviewing and monitoring security measures for effectiveness. Thus the Aeronautics Division did not minimize the business risk associated with its service provider's security measures and could have been unaware of any weaknesses at the service provider's data center that could have compromised the integrity and availability of MassDOT information.

Authoritative Guidance

Section DS2 of COBIT 4.1 states,

> *The need to assure that services provided by third parties . . . meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance.*

Reasons for Noncompliance

The Aeronautics Division does not have any formal policies and procedures that require a periodic review of security measures of the third-party Web-hosting service provider that supports Air-PORT.

c. The Aeronautics Division did not grant user access to Air-PORT based on business need.

The Aeronautics Division did not grant user access to Air-PORT based on business need. As a result, Air-PORT was vulnerable to alteration of information that could have affected business operations.

Our testing showed that (1) two external consultants had administrative privileges that, according to Aeronautics Division officials, were not based on business need; (2) five generic accounts that were used for testing had not been removed from the application; (3) one user account had not been removed immediately upon the user's termination; and (4) 21% of users were given administrative access to Air-PORT even though many of these users did not have a business need for this access based on their job responsibilities.

Authoritative Guidance

Section 3.1.1.2.7.4 of MassDOT's information security program (ISP) states,

> 1. *Each individual will be assigned a unique user account for accessing systems, network, and resources. These accounts and passwords shall not be group, shared or* ***generic*** [emphasis added]*. . . .*
>
> 5. *A quarterly (every three [3] months) review of all accounts, including remote access accounts, will be conducted to ensure that the accounts are still necessary and access rights are limited to the least privileges to meet business-need.*
>
> 6. *Procedures will be established for notification to relevant security administrators when a user's employment is terminated or job change results in access no*

> *longer being needed. Access for any terminated user will be immediately revoked.*

Reasons for Noncompliance

The Aeronautics Division did not establish a process with defined roles and responsibilities to review user access to Air-PORT.

d. The Aeronautics Division still had not documented and tested a business-continuity plan.

During our prior audit, we found that the Aeronautics Division had not documented and tested a business-continuity plan in conjunction with MassDOT IT to provide for the timely restoration of mission-critical and essential business functions. During our current audit, we found that the Aeronautics Division, in conjunction with MassDOT, still had not developed, documented, and tested a business-continuity plan that was appropriate to business and operational objectives, potential risks and exposures, and the relative importance of Aeronautics Division systems and data. Thus the Aeronautics Division had not assessed its ability to sustain operations in the event of a business interruption, which could have led to a loss or breach of data or an interruption of business.

The Aeronautics Division shares responsibility for business continuity with MassDOT IT; however, it is important that the division have adequate mechanisms to provide assurance that a business-continuity plan is in place and that its staff is sufficiently trained in performing recovery efforts for mission-critical applications such as Air-PORT.

Authoritative Guidance

The state Information Technology Division's Enterprise Business Continuity for IT Management Policy states,

> *Agencies are required to develop, implement, test and maintain a Business Continuity Plan (BCP) for all Information Technology Resources (ITR) that deliver or support core Critical Business Functions on behalf of the Commonwealth of Massachusetts. . . .*
>
> *Agencies are required to document, implement and annually test plans including the testing of all appropriate security provisions to minimize impact to systems or processes from the effects of major failures of IT Resources or disasters.*

Reasons for Noncompliance

The Aeronautics Division and MassDOT IT did not provide a reason for not having a business-continuity plan.

e. Aeronautics Division employees did not receive security-awareness training.

None of the Aeronautics Division's employees received the required security-awareness training. According to MassDOT's ISP,

> *Security Awareness Training identifies potential risks and vulnerabilities associated with MASSDOT information systems, reviews the user's role in protecting data confidentiality integrity and provides guidelines to protect against attacks on information systems. The Security Awareness Training also educates users about programs, directives and procedures and their role in safeguarding data.*

A lack of training in this area creates a higher-than-acceptable risk of inappropriate and unauthorized disclosure of the Aeronautics Division's information.

Authoritative Guidance

Section 6 of Executive Order 504, effective January 1, 2009, states,

> *All agency heads, managers, supervisors, and employees (including contract employees) shall attend mandatory information security training within one year of the effective date of this Order. For future employees, such training shall be part of the standardized orientation provided at the time they commence work. Such training shall include, without limitation, guidance to employees regarding how to identify, maintain and safeguard records and data that contain personal information.*

In addition, MassDOT's ISP states,

> *All employees, consultants, vendors, contractors, temporary staff and others with access to [personally identifiable information] and credit card data are required to complete basic Security Awareness Training upon hire and annually.*

Reasons for Noncompliance

MassDOT IT officials told us that because Air-PORT did not contain any personally identifiable information, it did not prioritize the development of security-awareness training for Aeronautics Division employees. However, the executive order is not limited to applications that contain personal information.

Recommendations

1. The Aeronautics Division should ensure that all future IT projects are staffed with personnel with expertise in IT project management. Further, IT projects should have detailed business and technical application requirements.

2. MassDOT should amend its Software Development & Maintenance Policy to require the involvement of MassDOT IT for Aeronautics Division–managed IT projects that MassDOT IT staff has adequate expertise to administer.

3. The Aeronautics Division should establish business requirements and a process to periodically review the effectiveness of its third-party service providers' security measures. The process should clearly define who is responsible for performing this review and should be defined in policies and procedures.

4. The Aeronautics Division should immediately remove all external consultants' accounts and test accounts from Air-PORT. MassDOT should establish a process to review the Air-PORT user accounts to ensure that access is based on business need. This process should clearly define the roles and responsibilities for performing the review.

5. The Aeronautics Division, in conjunction with MassDOT IT, should develop, document, and test a business-continuity plan in accordance with the Enterprise Business Continuity for IT Management Policy.

6. The Aeronautics Division should ensure that all employees receive security-awareness training upon hire and annually.

Auditee's Response

Mass DOT Aeronautics has purchased Aurigo Masterworks, a SSAE 16, SOC 2 compliant software package.

- *The software vendor is utilizing an Agile approach for implementation and professional services, with a fully trained, full-time, on-site team consisting of an experienced Project Manager (PM) and a Business Analyst (BA). The MassDOT Aeronautics Division has also engaged the services of a MassDOT IT Department PM and BA to ensure the project is delivered with a focus on internal controls. Additionally, the project team provides:*
  - *Established Steering Committee*
  - *Weekly Status Reviews*
  - *Architecture Review Board*

The Aurigo Masterworks IT project was procured after the completion of a detailed analysis and documentation of business and technical application requirements. . . .

The Aeronautics Division will have adequate roles and permissions via the Aurigo Masterworks software. The software application has been tested and certified by third parties to meet industry standard security measures and internal controls. Additionally, the Aeronautics Division will

provide adequate expertise and training for effective software administration. Moreover, the staff will leverage the MassDOT Software Development & Maintenance policy for guidance on software administration. . . .

The Aeronautics Division will adhere to the MassDOT Data Security policies and procedures for compliance of third-party service provider (TPSP) security reviews. The Aeronautics Division Administrator will appoint a staff member to assist DOT in the performance of the division TPSP reviews.

Additionally, AIR-Port will no longer be used by the Aeronautics Division; the Aurigo Masterworks application will replace the legacy system. The Aeronautics Division has deleted all external users of AIR-Port. . . .

The MassDOT Business Continuity Plan (BCP) is currently under development, including many related policies and procedures. The Aeronautics Division Administrator will document and test the BCP, and provide a policy mandating adherence of the BCP upon completion of the Plan and supporting policies. . . .

The Aeronautics Division will draft a policy mandating each employee complete security-awareness training annually, including compliance tracking. The Security and Awareness Training will be delivered in three phases: Phase 1—defines the program and establishes the approach for subsequent work this will occur between April and May; Phase 2—will launch training deliver online training according to plan and track and enforce compliance; Phase 3: will maintain the program and measure outcomes, repeat training and track and enforce compliance.

In addition to addressing our recommendations in its response, the Aeronautics Division provided information indicating that the Aurigo Masterworks software package cost $462,600.

2. The Aeronautics Division did not provide adequate oversight of reports used for aircraft registration or ensure that its aircraft database was complete and accurate.

The Aeronautics Division had inadequate controls over its aircraft registration process. Specifically, the division did not provide adequate oversight of airport managers' required semiannual reports, which are used for its aircraft registration process, and had significant control weaknesses in the completeness and accuracy of its aircraft registration database in Air-PORT. As a result, Air-PORT could not be updated and the number and type of commercial aircraft based at airports supported by the Aeronautics Division were not properly accounted for, which could affect the division's ability to make informed business decisions.

a. The Aeronautics Division did not provide adequate oversight of airport managers' required semiannual reports.

The Aeronautics Division did not effectively administer the collection of required information about aircraft based at the 36 airports it supports. As a result, Air-PORT information could not be updated, aircraft operating in the Commonwealth may not have been accounted for, and the Aeronautics Division could have lost revenue from unpaid aircraft registration fees. This revenue could have been used to address security and public safety risks.

The Aeronautics Division relies on airport managers to identify and report information about all civilian aircraft based at their airports. However, the division has not prescribed or standardized what information each airport needs to submit in these reports and does not routinely follow up with, or impose penalties on, airports that do not submit the reports. The Aeronautics Division uses information in these reports to verify and update information in Air-PORT. It is important to have an up-to-date database because the division bills aircraft owners based on the information in its database. During calendar year 2015, only 3 of 36 airport managers submitted the required semiannual reports, 18 provided only one of the two reports, and 15 did not file any reports.

Authoritative Guidance

Section 5.08(3)(f) of Title 702 of the Code of Massachusetts Regulations (CMR) requires that airport managers do the following:

> *Forward to the division, on March 1st and September 1st of each year, a listing of all aircraft based at the airport.*

As the oversight agency, the Aeronautics Division needs to take the measures necessary to ensure that its airports comply with this requirement. Best business practices would include establishing a standardized report to include all information needed regarding aircraft, routinely following up with airports that do not submit the reports, and imposing penalties on airports that do not submit the reports.

According to 702 CMR 5.09, the Aeronautics Division has the right to impose penalties on airport managers if they do not comply with 702 CMR.

Reasons for Noncompliance

During our audit period, the Aeronautics Division went through management changes and was in the process of defining new business processes for aircraft registration. Because of the management changes, staff members could not tell us why adequate oversight of airport managers' reports had not been established.

b. The Aeronautics Division lacked adequate monitoring and evaluation controls over the accuracy and completeness of its aircraft registration database.

The Aeronautics Division lacked adequate monitoring and evaluation controls over the accuracy and completeness of the information in its aircraft registration database. Because of the large number of aircraft in the database without a registration status and with other errors, it is impossible to verify that all aircraft were registered and all fees were billed and collected in 2015.

We tested the aircraft registration database in Air-PORT and found that it was inaccurate and incomplete. For example, testing of the database showed the following:

- over 900 records with a Federal Aviation Administration (FAA) number did not have a registration status
- 67 records did not have FAA numbers
- 3 records had invalid FAA numbers
- 307 records did not indicate where the aircraft was based
- 215 records did not note whether the aircraft was airworthy
- 82 aircraft were listed as having a gross weight of zero

We also identified data-entry errors in the database. Finally, in reviewing the reconciliation process between airport managers' reports and Air-PORT, we identified approximately 180 aircraft that were in the reports but had not been added to the Aeronautics Division's database.

Authoritative Guidance

Section ME2 of COBIT 4.1 states that, when monitoring and evaluating internal controls such as having accurate and complete information, organizations should identify weaknesses that cause

inaccurate and incomplete data, determine the causes of those weaknesses, report them to the appropriate personnel, and implement corrective actions.

Reasons for Noncompliance

During our audit period, the Aeronautics Division went through management changes and was in the process of defining new business processes for aircraft registration. Because of the management changes, staff members could not tell us why adequate oversight for monitoring and evaluating of database information had not been established. However, Aeronautics Division management believed that many of the issues occurred because legacy records were not removed from the database when data were transferred from the Airport Information Management System application to Air-PORT. In addition, the division did not have a reconciliation process between the total amount of aircraft registration fees recorded as having been collected in the state's Massachusetts Management Accounting and Reporting System (MMARS) and the amount recorded in Air-PORT.

Finally, the process established by the Aeronautics Division to add aircraft to Air-PORT from the airport managers' semiannual reports was deficient in that it required that an aircraft be added to the database only if it was listed as a valid registration on the FAA website at the time the report was being reconciled to Air-PORT. However, all aircraft based at airports should be added to Air-PORT because they could become registered with FAA and could affect the amount of federal funding each airport receives for airport improvements, which is based on airport demand.

Recommendations

1. The Aeronautics Division should establish formal policies and procedures to ensure that airport managers' reports are received twice a year. At a minimum, such policies and procedures should establish a standard report format, require following up with airports that do not submit the required reports, and establish penalties for noncompliance.

2. The Aeronautics Division should establish a process of periodic reporting to management that would identify aircraft without a registration status or with data-entry errors; reconcile the total amount of aircraft registration fees recorded as collected in MMARS and the amount recorded in Air-PORT; and ensure that all aircraft listed in airport managers' reports are in Air-PORT.

Auditee's Response

- *Management concurs with the auditors' comments, and the following action will be taken to improve the situation. Airport Managers are required to supply the Aeronautics*

Division with a current Based Aircraft List twice a year on March 1 and September 1. The Aeronautics Division Director of Administration and Finance will ensure that notice is sent to each individual airport manager in February and August of each year to submit their airport list in compliance with Code of Massachusetts Regulations (CMR) 702, Section 5.08.

The Aeronautics Division Director of Administration and Finance, Aeronautics Aeronautical Inspector and the Aeronautics Registration Accountant will maintain a current list of all respondents and follow up to ensure all airport managers are complaint with their submission. All delinquent non-responders will be notified directly from the Aeronautics Division Director of Administration and Finance. The Aeronautics Division Finance Department Policies and Procedures Manual will be updated with the associated formal policies and procedures and staff will be advised of all revisions.

- *For all non-Primary airports in the National Plan of Integrated Airport System (NPIAS) they will enter, update and confirm a listing of based aircraft in the Federal Aviation Administration (FAA) National Based Aircraft Inventory Program database at www.basedaircraft.com and notify the Aeronautics Division Director of Administration and Finance and the Aeronautics Aeronautical Inspector via email.*

    - *All other airports will update the based aircraft list on a provided excel spreadsheet and submit the completed spreadsheet to the Aeronautics Division Director of Administration and Finance and the Aeronautics Aeronautical Inspector. . . .*

- *The Aeronautics Division identified system limitations with the AIR-Port Aircraft Registration module and decided to replace the module. The Aeronautics Division entered into an agreement with Aurigo Software Technologies, Inc. to implement their Masterworks platform to automate, standardize and modernize the Aircraft Registration processes. This includes: identification of aircraft without a registration status, data validation to entry minimize errors, tracking of aircraft registration fees, MMARS integration for accurate reconciliation of collected fees, enhanced form generation, account management, revenue managements, dunning and [ad hoc] querying.*

  The Aeronautics Division Director of Administration and Finance will develop the policies and procedures (consistent with the implementation timeline) to ensure they address all items listed in the Recommendation. The Aeronautics Division Finance Department Policies and Procedures Manual will be updated with the associated policies and procedures and staff will be advised of all revisions.

  Prior to the Masterworks implementation the Aeronautics Division Director of Administration and Finance will work to ensure timely account management reporting; perform the three-way revenue reconciliation with the AIR-Port, Bank Of America depositary account and the MMARS revenue account. In addition, the Aeronautics Division Director of Administration and Finance will ensure the Aircraft Registration program is compliant with all promulgated laws, regulations and procedural guidance.