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

Official Audit Report – Issued March 23, 2017

# Division of Banks

For the period July 1, 2014 through June 30, 2016

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

March 23, 2017

Mr. Terence A. McGinnis, Commissioner of Banks
Division of Banks
1000 Washington Street, 10th Floor
Boston, MA 02118

Dear Commissioner McGinnis:

I am pleased to provide this performance audit of the Division of Banks. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2014 through June 30, 2016. My audit staff discussed the contents of this report with management of the division, whose comments are reflected in this report.

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

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

# TABLE OF CONTENTS

# LIST OF ABBREVIATIONS

| | |
|---|---|
| AML | anti-money-laundering |
| BCP | business-continuity plan |
| CMR | Code of Massachusetts Regulations |
| COOP | continuity-of-operations plan |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission |
| DOB | Division of Banks |
| DRP | disaster-recovery plan |
| EOHED | Executive Office of Housing and Economic Development |
| ERM | enterprise risk management |
| FinCEN | Financial Crimes Enforcement Network |
| FTA | foreign transmittal agency |
| ICP | internal control plan |
| ICQ | Internal Control Questionnaire |
| OCABR | Office of Consumer Affairs and Business Regulation |
| OSA | Office of the State Auditor |
| OSC | Office of the State Comptroller |
| OST | Office of the State Treasurer |

# EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of certain activities of the Division of Banks (DOB) for the period July 1, 2014 through June 30, 2016. In this performance audit, we examined DOB activities related to the licensing and oversight of foreign transmittal agencies (FTAs),[1] including processes in place to ensure that FTAs filed required surety bonds, complied with record-retention requirements, and implemented effective anti-money-laundering programs in accordance with federal laws and regulations.

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

| | |
|---|---|
| **Finding 1**<br>**Page 8** | DOB does not confirm that FTAs conducting business in Massachusetts maintain three years' worth of records. |
| **Recommendations**<br>**Page 9** | 1. DOB should require its examiners to verify that licensees maintain three years' worth of records in accordance with applicable statutory and regulatory requirements and should communicate this requirement to its examiners.<br>2. DOB should follow up with the licensee whose policies did not define a record-retention period to ensure that it updates its policies to include this information. |
| **Finding 2**<br>**Page 10** | DOB's internal control plan (ICP) has not been updated as required and lacks critical components of internal control. |
| **Recommendation**<br>**Page 11** | DOB should ensure that it adheres to all of the requirements of the Office of the State Comptroller (OSC) for developing and maintaining its ICP. If necessary, DOB should continue to seek out training opportunities and guidance from OSC on this matter. |
| **Finding 3**<br>**Page 11** | DOB did not immediately report unaccounted-for losses of property to OSA. |
| **Recommendations**<br>**Page 12** | 1. DOB should ensure that all unaccounted-for losses are immediately reported to OSA.<br>2. DOB should update its ICP to include the immediate-reporting requirement and ensure that the requirement is communicated to its employees.<br>3. When necessary, DOB should seek advice and clarification from OSC about questions on its Internal Control Questionnaire before completing it and submitting it to OSC. |

1. FTAs receive funds from consumers for transfer to recipients located in foreign countries.

# OVERVIEW OF AUDITED ENTITY

The Division of Banks (DOB) is authorized by Section 1 of Chapter 26 of the Massachusetts General Laws and operates under the direction of a Commissioner of Banks who is appointed by the Governor.[2] DOB is a division of the Office of Consumer Affairs and Business Regulation (OCABR), which is within the Executive Office of Housing and Economic Development (EOHED). DOB is responsible for the supervision and regulation of non-banking financial-service providers, which as of December 31, 2015 comprised 8,071 money-service businesses,[3] consumer-finance companies,[4] debt collectors, mortgage companies, and mortgage-loan originators with a combined 4,398 branch and agent locations. DOB also oversees state-chartered banks and credit unions, which as of December 31, 2015 totaled 189 institutions with 1,247 branch office locations holding $383.1 billion in total assets.[5] The division received state appropriations of $18,543,118 and $18,843,118 in fiscal years 2015 and 2016, respectively.[6]

DOB has four units: Non-depository Institution Supervision, Depository Institution Supervision, Enforcement and Investigation, and Administration. A policy group chaired by the Commissioner of Banks and consisting of DOB senior management oversees all regulatory matters, conducts strategic planning, and directs day-to-day operations. OCABR's Administrative Services Unit performs most of the financial and accounting functions for DOB. DOB's information technology is managed and maintained by the EOHED Information Technology Department.

During our audit period, DOB had approximately 160 employees, including bank examiners, managers, and support employees. Its headquarters are located at 1000 Washington Street in Boston, and it has field offices in Burlington, Lakeville, and Springfield.

2. A transition of the Commissioner of Banks occurred during our audit.
3. Money-service businesses are foreign transmittal agencies, check sellers, or check cashers.
4. Consumer finance companies are non-bank lenders that offer small loans to consumers, typically to finance the purchase of goods or services.
5. Statistical information is from the DOB website at http://www.mass.gov/ocabr/docs/dob/dobataglance.pdf (accessed December 31, 2015).
6. DOB's fiscal year 2015 appropriation of $19,143,118 was reduced to this amount by budgetary cuts and consisted of direct appropriations of $16,193,118 and retained revenue of $2,350,000. DOB's fiscal year 2016 appropriation consisted of direct appropriations of $16,493,118 and retained revenue of $2,350,000.

# AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of certain activities of the Division of Banks (DOB) for the period July 1, 2014 through June 30, 2016.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and 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, if applicable, where each objective is discussed in the audit findings.

| Objective | Conclusion |
|---|---|
| 1. Does DOB ensure that foreign transmittal agencies (FTAs) properly calculate the amount of the bond required as a condition of licensure per Section 2 of Chapter 29 of the General Laws[7] and ensure that bonds are approved and filed per Section 3 of Chapter 169 of the General Laws?[8] | **Yes** |
| 2. Does DOB ensure that FTAs maintain three years' worth of records in accordance with Section 10 of Chapter 169 of the General Laws? | **No; see Findings 1 and 3** |
| 3. Does DOB ensure that FTAs establish effective anti-money-laundering (AML) programs as required by regulations related to the federal Bank Secrecy Act? | **Yes** |

In addition, in the course of our audit work, we determined that DOB did not update its internal control plan (ICP) or conduct annual risk assessments for fiscal years 2015 and 2016 (Finding 2). We also followed up on a finding from a prior audit (No. 2011-0100-7T) related to DOB's business continuity plan and management's corrective action and found that management had not completely addressed the finding (Other Matters).

7. Surety bonds must be in the amount of $50,000 or twice the weekly average of currency transmitted to foreign countries (whichever is greater).
8. Surety bonds must be approved by the Commissioner of Banks and the State Treasurer and filed with the Office of the State Treasurer.

To achieve our audit objectives, we gained an understanding of the internal controls we determined to be relevant to our audit objectives and tested the controls' operating effectiveness over the following areas: surety bonds, record retention, and AML programs. We conducted further audit testing as described in the following subsections.

## Surety Bonds

FTAs must be licensed by DOB to operate in Massachusetts. During our audit period, there were 60 FTAs operating in the Commonwealth. Section 2 of Chapter 169 of the General Laws requires an FTA to submit a surety bond to DOB for consumer protection against the FTA's insolvency, bankruptcy, or failure to transfer funds. The surety bond must be in the amount of $50,000 or twice the weekly average of currency transmitted to foreign countries (whichever is greater).[9]

To gain an understanding of DOB's surety bond compliance practices, we reviewed its ICP and related policies and procedures. We also interviewed DOB management and staff members who were responsible for FTA licensing and the oversight of the surety bond process.

DOB ensures that surety bonds are for the correct amounts, approved by the Commissioner of Banks and the State Treasurer, and filed with the Office of the State Treasurer (OST) during three distinct processes within the licensing lifecycle:

1. Initial licensing—DOB must receive a $50,000 surety bond from FTAs when their licenses are approved, before they conduct business in the Commonwealth.
2. License renewal—Annually, DOB processes FTA license-renewal applications; this processing includes a validation of the appropriateness of the amount of the surety bond on file.
3. FTA examinations—Periodically, DOB examines FTAs to verify that FTA surety bond amounts are appropriate through an analysis of FTA currency transmittal records.

To test surety bond compliance during these three processes, we selected samples from the 60 FTAs regulated by DOB during the audit period and reviewed each one for the applicable processes in which it participated, as follows:

1. Initial licensing—We randomly selected 6 of the 17 FTAs that became licensed during the audit period. We reviewed the surety bonds submitted by these licensees to verify that they were for

9. FTAs are responsible for adjusting the value of their sureties as transaction volume dictates. At the time of the initial bond, since no currency has yet been transmitted to foreign countries, the bond is set at $50,000.

the required $50,000, were approved, and were filed in accordance with Section 3 of Chapter 169 of the General Laws. Additionally, we verified that each surety bond's effective date was on or before the date the Commissioner of Banks issued a letter authorizing the FTA to conduct business in the Commonwealth.

2. License renewal—We randomly selected 19 of the 58 FTAs that submitted license-renewal applications for calendar year 2016. We obtained the FTA renewal applications' supporting documentation and reconciled the surety bond calculations to the surety bond amounts on file with OST.

3. FTA examinations—We randomly selected 11 of the 33 FTAs that DOB examined during the audit period. We obtained the surety bond calculations from DOB's supporting documentation for its examinations and reconciled the calculated amounts to the amounts of the surety bonds on file with OST.

## 1. Record Retention

### a. Foreign Transmittal Agency Record Retention Requirements

The US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) requires FTAs to file reports on certain transactions and maintain supporting documentation.[10] FinCEN analyzes these reports to support law-enforcement efforts and to identify money-laundering developments, trends, and patterns. DOB analyzes samples of transaction records during examinations to assess FTA compliance with these reporting and recordkeeping requirements. DOB requires appropriate and timely corrective action on any reporting or recordkeeping issues. Serious violations could cause an FTA to lose its operating license.

To gain an understanding of DOB's process for ensuring that FTAs retain records in accordance with state and federal laws, we reviewed DOB's ICP and related policies and procedures and interviewed DOB management and staff members who were responsible for FTA oversight. DOB indicated that it reviews FTA record-retention policies during the initial licensing process and during examinations.

We selected a random sample of 10 of the 22 FTAs that were licensed for at least three years and were examined by DOB[11] at least once during the audit period. DOB managers told us the three-year record-retention requirement was not explicitly addressed as part of the division's examination process. DOB does verify that FTAs have record-retention procedures; therefore, we reviewed

10. See the appendix to this report for a summary of federal reporting and recordkeeping requirements.
11. DOB selects FTAs using a risk-based approach. Consequently, the time between examinations can vary. However, from OSA's review of records, it appeared that the amount of time between examinations is typically less than two years.

examination records for evidence of this verification. Additionally, we obtained the procedures for the sample of 10 FTAs and verified the procedures' adequacy.

### b. Chapter 647 Filing Requirements

The Chapter 647 of the Acts of 1989 law requires state agencies to immediately file a report with OSA if any "unaccounted for variances, losses, shortages, or thefts of funds property" are identified. We reviewed the ICP to determine whether the Chapter 647 reporting requirements were defined therein, and reviewed the Internal Control Questionnaire submitted to the Office of the State Comptroller for fiscal years 2015 and 2016, to verify the accuracy of management's representation related to Chapter 647 filings.

## 2. AML

### a. AML Programs

DOB must ensure that FTAs comply with the Bank Secrecy Act, which Congress enacted in 1970 to minimize the risk of money laundering, fraud, and financing of terrorist activities. Section 1022.210 of Title 31 of the Code of Federal Regulations dictates how this act is to be implemented.

To comply with the Bank Secrecy Act, an FTA must develop and implement an AML program that consists of the following four pillars:

1. documented policies, procedures, and internal controls related to verifying customer identification, filing reports, creating and retaining records, and responding to law-enforcement requests
2. designation of an AML compliance officer
3. implementation of an AML training program
4. evidence of independent AML program reviews

To gain an understanding of DOB's process for ensuring that FTAs complied with AML program requirements, we reviewed DOB's ICP and related policies and procedures. We also interviewed DOB managers and other staff members who were responsible for verifying that FTAs comply with AML program requirements.

DOB assesses the establishment of AML programs during initial licensing and assesses program effectiveness during examinations of FTAs. DOB examination reports are very detailed with respect

to the review of AML programs. The examination reports refer to each of the four pillars of AML programs and document how licensees fulfill the requirements. For example, the reports identify the AML compliance officers, outline the training programs, and include evidence of independent review.

### b. AML Program Establishment

To determine whether DOB ensured that FTAs established AML programs at the time of initial licensure, we selected a random sample of 10 out of a population of the 17 companies that became licensed during our audit period. We reviewed DOB's FTA licensing files to verify that DOB had an AML program on file for each FTA and that each program addressed the four pillars of AML programs.

### c. AML Program Effectiveness

To determine whether DOB ensured the effectiveness of FTAs' AML programs, we selected a random sample of 10 out of a population of the 33 companies that DOB examined during our audit period. We reviewed examination reports to verify that DOB assessed the FTAs' AML programs to ensure that they effectively addressed the four pillars of AML programs.

## 3. Data Reliability

We obtained the source documents that we would use during testing from files maintained on the DOB computer network. To assess network access to DOB's shared public folders, we tested certain general information-technology controls using questionnaires, interviews, and observations. During our testing, we examined specific documents, such as the Internal Reports to the Commissioner, which detail FTAs' AML programs; examination reports, which include complete assessments of licensees' compliance; and licensee annual reports and other source documents. We determined that the data were sufficiently reliable for the purposes of audit testing.

Whenever sampling was used, we applied a nonstatistical approach, and as a result, we were not able to project our results to the entire populations.

# DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

## 1. The Division of Banks does not confirm that foreign transmittal agencies conducting business in Massachusetts maintain three years' worth of records.

The Division of Banks (DOB) does not require its examiners to verify that foreign transmittal agencies (FTAs) conducting business in Massachusetts maintain the statutorily required three years' worth of records. Instead, DOB examiners review licensees' recordkeeping policies and analyze a sample of records, typically only 12 months as opposed to the 36 months that would be necessary to properly assess compliance with recordkeeping requirements. Further, of the 10 FTA licensees whose records we sampled (out of 17 that became licensed during the audit period), 1 did not have a policy that clearly defined the required record-retention period.

If DOB does not require its examiners to verify that FTAs retain all of the required records, in the Office of the State Auditor's (OSA's) opinion, there is a higher-than-acceptable risk that an FTA's compliance with statutory and regulatory requirements (such as those dealing with consumer protection and anti-money-laundering activities) is unsupported and that instances of noncompliance will therefore go undetected.

### Authoritative Guidance

Section 10 of Chapter 169 of the Massachusetts General Laws requires FTA licensees to maintain three years' worth of records to allow the Commissioner of Banks to determine whether they are complying with Chapter 169 and any other applicable laws, rules, and regulations. Section 48 of Title 209 of the Code of Massachusetts Regulations (CMR) defines procedures by which FTAs should comply with Chapter 169; it also sets forth record-retention requirements for each customer transaction. Section 44 of Title 209 of the CMR establishes procedures for DOB to use to verify that FTAs comply fully with the record-retention provisions of Chapter 169.

### Reasons for Noncompliance

DOB management indicated that it interpreted the recordkeeping requirement solely as a tool to cite licensees with violations if records reviewed and/or requested by DOB were inadequate, were never created, or had been destroyed. DOB added that current transaction analyses conducted during

examinations were sufficient to identify any licensee recordkeeping issues. However, DOB's current procedures would only identify issues within its sample of records, typically 12 months.

## Recommendations

1. DOB should require its examiners to verify that licensees maintain three years' worth of records in accordance with applicable statutory and regulatory requirements and should communicate this requirement to its examiners.

2. DOB should follow up with the licensee whose policies did not define a record-retention period to ensure that it updates its policies to include this information.

## Auditee's Response

*The Division's current examination practices include review and testing to verify that licensees create and maintain all required records. The focus of this review is to ensure that licensees maintain books, records and accounts in a manner that will allow the Commissioner to determine whether the licensee is complying with applicable state and federal laws and regulations. Division examiners are well trained and quite familiar with these requirements.*

*Each of the examinations conducted during the scope of the audit included a review of the licensee's record-keeping practices. The Division's standard document request list template for foreign transmittal exams requires each licensee to produce a copy of their record retention schedule and record retrieval procedures. As noted in the Division's Foreign Transmittal Examination Workprogram, the examiners are instructed to confirm the licensee preserves its records for a minimum of three years in compliance with the state record-keeping requirements and for the minimum five-year retention period in compliance with federal BSA record-keeping requirements.*

*In practice, this review has focused on verifying each licensee maintains appropriate record-keeping policies and interviewing compliance staff to confirm they are familiar with state and federal record-keeping requirements. . . . Division examiners also conduct transactional testing and data integrity reviews to verify that each licensee is creating proper records. . . .*

*However, while the division believes its current practices are appropriate and have been effective in ensuring Licensees maintain adequate records, the Division is expanding its transaction testing of remittance records to ensure that licensees are maintaining records for a full three years as required by state law. . . . The Division has memorialized this in its Foreign Transmittal Examination Workprogram and communicated this to examiners.*

*In regard to the Licensee whose policies did not directly address the specific period of time during which records would be maintained (it included only a generic reference to maintaining records for the minimum period required by law), the Division has already reached out to the Licensee in question to obtain an updated copy of its record retention policy to confirm it accurately reflects the minimum record retention periods for both state and federal law. If it does not specify the accurate record retention periods, the Division will instruct the Licensee to update its policy accordingly.*

## Auditor's Reply

Although the division's Foreign Transmittal Examination Workprogram instructs examiners to confirm that licensees preserve their records in compliance with the applicable state and federal recordkeeping requirements, in practice DOB does not actually verify that they do so. Rather, as noted above, DOB only samples the licensee's records during examinations. In OSA's opinion, this process needs to be improved to ensure that licensees fully comply with the applicable record-retention requirements. Based on its response, DOB is taking appropriate measures to address our concerns in this area.

## 2. DOB's internal control plan has not been updated as required and lacks critical components of internal control.

DOB's internal control plan (ICP), an agency-wide document that summarizes risks and controls for all of its business processes, is not updated annually; it was last updated in June 2014. In addition, the ICP does not consider, or adequately address, three critical components of enterprise risk management (ERM) as required by the Office of the State Comptroller (OSC): objective setting, risk assessment, and monitoring. Specifically, although the ICP did contain some objectives, they were not specific or measurable objectives that would help DOB to complete its mission; the ICP did not identify specific risks, as needed in order to develop effective internal control procedures; and the ICP did not include ways to monitor and evaluate the effectiveness of controls.

The absence of an up-to-date, comprehensive ICP that incorporates the critical components of ERM may hinder DOB's ability to achieve its mission and objectives effectively, efficiently, and in compliance with applicable laws, rules, and regulations.

## Authoritative Guidance

In its document *Enterprise Risk Management—Integrated Framework*, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM as "a process, effected by the entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage the risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." To comply with OSC internal control guidelines, an ICP must contain information on the eight components of ERM: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. COSO guidance states

that in order to be effective, all components of an internal control system must be present, be functioning properly, and be operating together in an integrated manner.

In addition, OSC's Internal Control Guide requires that an ICP be updated as often as changes in management, level of risk, program scope, and other conditions warrant, but at least annually.

## Reasons for Noncompliance

DOB management stated that updating the ICP and ensuring that it addressed all the components of ERM were not a priority. Management has since attended internal control training offered by OSC, and it is now in the process of updating the ICP.

## Recommendation

DOB should ensure that it adheres to all of OSC's requirements for developing and maintaining its ICP. If necessary, DOB should continue to seek out training opportunities and guidance from OSC on this matter.

## Auditee's Response

*The Division acknowledged as part of its Internal Control Questionnaire (ICQ) submission in June 2016 that it had not updated the Internal Control Plan (ICP) in FY16. The Division has consistently had an individual (or individuals) assigned to review the ICP and submit the annual ICQ; however for FY16, the ICP was reviewed and in the process of being updated—a process which had not yet been completed during the audit period. As part of the ICQ submission, and consistent with [OSA's] recommendation in this audit, the Division is in the midst of updating the ICP for FY17. The Division will incorporate [OSA's] suggestion to ensure that the ICP addresses critical components of enterprise risk management in accordance with the Office of the State Comptroller's guidance. The Division will fully document both reviews and updates of the ICP accordingly going forward as required.*

## 3. DOB did not immediately report unaccounted-for losses of property to OSA.

Three laptops, each with an estimated value of $200, were determined to be missing in summer 2015 but not reported to OSA as missing until June 28, 2016. This was in spite of DOB indicating in its Internal Control Questionnaires (ICQs) submitted to OSC for fiscal years 2015 and 2016 that all instances of lost property were immediately reported to OSA. Not immediately reporting losses to OSA can prevent or delay an independent assessment of potential internal control weaknesses that may have contributed to

or caused the issue. Further, inaccurate information on the ICQ prevents OSC from effectively assessing the adequacy of DOB's internal control system.

## Authoritative Guidance

Chapter 647 of the Acts of 1989 requires state agencies and departments to immediately report unaccounted-for losses of property to OSA.

The ICQ is a document designed by OSC that is sent to departments each year requesting information and department representations on their internal controls. The purpose of the ICQ is to provide an indication of the effectiveness of a department's internal controls and, along with other considerations, is used by external auditors to render an opinion on a department's internal controls.

## Reasons for Noncompliance

DOB management indicated that the division did not immediately report the loss of the three laptops, and incorrectly responded to the ICQ, because management did not understand Chapter 647's reporting requirement. In addition, DOB's ICP did not clearly define the need to report Chapter 647 losses immediately to OSA.

## Recommendations

1. DOB should ensure that all unaccounted-for losses are immediately reported to OSA.
2. DOB should update its ICP to include the immediate-reporting requirement and ensure that the requirement is communicated to its employees.
3. When necessary, DOB should seek advice and clarification from OSC on ICQ questions before completing its ICQ and submitting it to OSC.

## Auditee's Response

*For the specific case of the three laptops in question, the affirmative ICQ response (unaccounted-for variances are submitted immediately) was logged on June 14, 2016—a submission at the time intended to be a truthful response—two weeks prior to the Chapter 647 submission on June 28, 2016. As per the C647 filing, three laptops were determined to be missing in the summer months of 2015 as part of a computer lease refresh. Signed records indicated that two of the three laptops were returned by Division employees to the centralized IT department. The Division delayed the C647 report pending a bona fide exhaustive search effort to determine whether the equipment was in fact missing (the Division had deferred to centralized IT department's review of inventory/implementation of IT tracking system to confirm accounting of all equipment—a process which ran through the end of FY16). The Division acknowledges that a C647 filing should*

*have occurred in the summer months of 2015 when initial indication suggested that the laptops might be missing.*

*Going forward, the Division will incorporate [OSA] recommendations to ensure that C647 filings are immediate (regardless of a search effort to locate, the unaccounted-for equipment must be reported as soon as it is known to be missing); efforts to ensure compliance will include clear statement in the ICP and notification to all employees of the importance of this requirement.*

# OTHER MATTERS

## The Division of Banks should develop a business-continuity plan.

During a prior audit (No. 2011-0100-7T), the Office of the State Auditor (OSA) found that the Division of Banks (DOB) did not have a formal business-continuity plan (BCP)[12] or disaster-recovery plan (DRP)[13] to provide reasonable assurance that information-technology functions could be regained effectively and in a timely manner if a disaster rendered its automated systems inoperable. Additionally, DOB had not implemented a continuity-of-operations plan (COOP),[14] but did have a draft dated February 2011.

The Massachusetts Office of Information Technology's Enterprise Business Continuity for IT Management Standards, dated June 5, 2013, require each executive-department agency to implement a BCP, DRP, and COOP. These plans must be tested annually, and training must be provided to people who execute and participate in the plans. Annual testing is necessary to highlight weaknesses in the plans and to allow management to improve the plans continuously.

Although they were not part of our audit objectives, during our audit fieldwork we asked DOB for its BCP, DRP, and COOP. No BCP was available; however, we did receive a DRP (last updated in April 2015) and a copy of a COOP (which was implemented and last tested in June 2013). DOB should develop and implement a BCP to identify potential risks that could affect systems or services that support critical business functions and to develop strategies to mitigate potential threats to business operations. DOB should conduct annual testing and training to ensure that the BCP, DRP, and COOP are effective and that personnel who are responsible for implementing the plans are sufficiently familiar with the processes to execute the plans effectively in the event of a disaster.

## Auditee's Response

> *In addition to the ICP plan update that is underway, the Division is also in the process of updating the Continuity of Operations Plan (COOP) and planning for a test of the plan. Further, as [OSA] indicated in the "Other Matters" section of this report, the Division will clearly identify per Massachusetts Office of Information Technology's Enterprise Continuity for IT Management a Business Continuity Plan, a Disaster Recovery Plan, and the COOP.*

12. A BCP is a plan that develops risk-based strategies to mitigate identified potential threats to business operations. At a minimum, it should include a DRP and COOP.
13. A DRP is an information-system-based plan designed to allow for quick recovery of critical systems, applications, and information-technology infrastructure in the event of a large-scale disaster.
14. A COOP is a plan that is to be invoked under a DRP if business operations need to be relocated.

# APPENDIX

The following is an excerpt from *A Quick Reference Guide for Money Services Businesses*, a guide issued by the Financial Crimes Enforcement Network within the US Department of the Treasury. (This type of business includes foreign transmittal agencies.)

> *The [federal Bank Secrecy Act]'s reporting and recordkeeping provisions apply to banks, savings and loans, and credit unions as well as other financial institutions, including money services businesses (MSBs).*
>
> ***Currency Transaction Reports***
>
> *MSBs must file a Currency Transaction Report (CTR) within 15 days whenever a transaction or series of transactions in currency:*
>
> - *Involves more than $10,000 in either cash-in or cash-out,* ***and***
> - *Is conducted by, or on behalf of, the same person,* ***and***
> - *Is conducted on the same business day.*
>
> *Multiple cash transactions are considered to be one transaction on which a CTR must be filed if the MSB has knowledge that:*
>
> - *They are by or on behalf of the same customer during one business day,* ***and***
> - *They are conducted at one or more branches or agents of the same MSB,* ***and***
> - *They total more than $10,000 in either cash-in or cash-out. . . .*
>
> ***Money Transfers of $3,000 or More***
>
> *MSBs that provide money transfer services must obtain and record specific information for each money transfer of $3,000 or more, regardless of the method of payment. . . . Keep the record for 5 years from the date of transaction. . . .*
>
> ***Suspicious Activity Reporting Requirements***
>
> *Certain money services businesses—businesses that provide money transfers or currency dealing or exchange; or businesses that issue, sell, or redeem money orders or traveler's checks—must report suspicious activity involving any transaction or pattern of transactions at or above a certain amount:*
>
> - *$2,000 or more;*
> - *$5,000 or more for issuers reviewing clearance records.*

*You have 30 calendar days to file a [Suspicious Activity Report] after becoming aware of any suspicious transaction that is required to be reported.*