



# Office of Inspector General

November 2007  
Report No. AUD-08-003

---

**FDIC's Implementation of the  
USA PATRIOT Act**

**AUDIT REPORT**

*Office of Audits*



**oig**

## TABLE OF CONTENTS

<b>BACKGROUND</b>	<b>2</b>
<b>RESULTS OF AUDIT</b>	<b>7</b>
<b>IMPLEMENTATION OF EXAMINATION PROCEDURES FOR CUSTOMER IDENTIFICATION PROGRAMS</b>	<b>8</b>
<b>Requirements Related to the CIP</b>	<b>9</b>
<b>Identification of Apparent Violations</b>	<b>9</b>
<b>Conclusion</b>	<b>12</b>
<b>Recommendation</b>	<b>13</b>
<b>IMPLEMENTATION OF EXAMINATION PROCEDURES FOR RISK ASSESSMENTS</b>	<b>13</b>
<b>Examination Guidance for Risk Assessments</b>	<b>13</b>
<b>Institution Preparation and Examiner Evaluations of Risk Assessments</b>	<b>15</b>
<b>Use of Appendix J in the FFIEC BSA/AML Examination Manual for Assessing Risk</b>	<b>16</b>
<b>Recommendation</b>	<b>17</b>
<b>CORPORATION COMMENTS AND OIG EVALUATION</b>	<b>17</b>
<b>APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY</b>	<b>19</b>
<b>APPENDIX II: STATUS OF REGULATIONS AND EXAMINATION PROCEDURES FOR PATRIOT ACT REQUIREMENTS</b>	<b>26</b>
<b>APPENDIX III: CUSTOMER IDENTIFICATION PROGRAM REQUIREMENTS</b>	<b>28</b>
<b>APPENDIX IV: CORPORATION COMMENTS</b>	<b>30</b>
<b>APPENDIX V: MANAGEMENT RESPONSE TO RECOMMENDATIONS</b>	<b>32</b>
<b>TABLES</b>	
<b>Table 1: Status of Examination Procedures for PATRIOT Act Provisions</b>	<b>3</b>
<b>Table 2: Supervisory and Enforcement Actions for Noncompliance with BSA/AML and PATRIOT Act Requirements</b>	<b>4</b>
<b>Table 3: Apparent CIP Violations</b>	<b>11</b>
<b>Table 4: The FDIC's Activities to Address the Government Performance and Results Act</b>	<b>22</b>
<b>Table 5: Synopsis of FDIC OIG Prior Audit Coverage of BSA and PATRIOT Act Compliance</b>	<b>23</b>
<b>FIGURES</b>	
<b>Figure 1: Risk Assessment Link to the BSA/AML Compliance Program</b>	<b>6</b>
<b>Figure 2: Risk Categories That Should be Considered During the Risk Assessment Process</b>	<b>14</b>

## ACRONYMS

<b>AML</b>	<b>Anti-Money Laundering</b>
<b>BSA</b>	<b>Bank Secrecy Act</b>
<b>C&amp;D</b>	<b>Cease and Desist Order</b>
<b>C.F.R.</b>	<b>Code of Federal Regulations</b>
<b>CIP</b>	<b>Customer Identification Program</b>
<b>CMP</b>	<b>Civil Money Penalty</b>
<b>CSBS</b>	<b>Conference of State Bank Supervisors</b>
<b>DSC</b>	<b>Division of Supervision and Consumer Protection</b>
<b>FBA</b>	<b>Federal Banking Agency</b>
<b>FDI</b>	<b>Federal Deposit Insurance</b>
<b>FFIEC</b>	<b>Federal Financial Institutions Examination Council</b>
<b>FIL</b>	<b>Financial Institution Letter</b>
<b>FinCEN</b>	<b>Financial Crimes Enforcement Network</b>
<b>GAO</b>	<b>Government Accountability Office</b>
<b>HIDTA</b>	<b>High Intensity Drug Trafficking Area</b>
<b>HIFCA</b>	<b>High Intensity Financial Crimes Area</b>
<b>MOU</b>	<b>Memorandum of Understanding</b>
<b>OFAC</b>	<b>Office of Foreign Assets Control</b>
<b>OIG</b>	<b>Office of Inspector General</b>
<b>ONDCP</b>	<b>Office of National Drug Control Policy</b>
<b>PATRIOT Act</b>	<b>Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001</b>
<b>RD</b>	<b>Regional Directors</b>
<b>ROE</b>	<b>Report of Examination</b>
<b>TIN</b>	<b>Taxpayer Identification Number</b>
<b>U.S.C.</b>	<b>U.S. Code</b>
<b>ViSION</b>	<b>Virtual Supervisory Information on the Net</b>



## *FDIC's Implementation of the USA PATRIOT Act*

### Results of Audit

#### Background and Purpose of Audit

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act) was signed into law on October 26, 2001. The Patriot Act made a number of amendments to the anti-money laundering (AML) provisions of the Bank Secrecy Act (BSA) of 1970, which was passed to prevent banks and other financial service providers from being used in criminal activity and to identify the source, volume, and movement of currency and other monetary instruments into or out of the United States or deposited in financial institutions. In addition, the Patriot Act expands the Treasury Department's authority to regulate the activities of U.S. financial institutions, particularly their relations with individuals and entities with foreign ties. The Patriot Act requires financial institutions to implement a written, board-approved Customer Identification Program (CIP) that is appropriate for the institution's size and type of business.

In June 2005, the Federal Financial Institutions Examination Council (FFIEC), which includes the FDIC and other federal banking agencies, issued interagency guidance in the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual*. The manual updates examination procedures for BSA/AML and Patriot Act compliance and emphasizes the importance of a BSA/AML risk assessment.

The audit objectives were to determine whether (1) examination procedures are designed to evaluate institution compliance with the AML and terrorist financing provisions of the Patriot Act and (2) those procedures were fully and consistently implemented to provide reasonable assurance that institutions with weak programs for detecting money laundering and terrorist financing activity will be identified and appropriate corrective measures taken.

The FDIC, in conjunction with the FFIEC, has issued comprehensive examination procedures in the FFIEC BSA/AML Examination Manual designed to assist examiners in evaluating institution compliance with the AML and terrorist financing provisions of the Patriot Act. Additionally, the FDIC has issued supervisory and enforcement guidance on corrective actions for noncompliance with the BSA and Patriot Act and referrals of significant BSA violations for possible assessment of civil and/or criminal penalties. The FDIC has taken action in a number of cases to address noncompliance with BSA and Patriot Act provisions and related regulations. The FDIC has also taken steps to strengthen BSA and Patriot Act compliance, including training and industry outreach, certifications for AML specialists, and establishment of BSA-related performance measures.

Generally, FDIC examiners implemented examination procedures in the FFIEC BSA/AML Examination Manual related to the Patriot Act. However, the FDIC could enhance the implementation of examination procedures with respect to CIPs. The FDIC examiners reviewed CIPs for all 24 of our sampled financial institutions and cited CIP-related violations at 5 of those institutions. However, we found other apparent violations of CIP requirements that were not identified and reported by examiners. The CIP requirements are intended to ensure that a financial institution can form a reasonable belief that it knows the true identity of its customers. Consistent examiner identification and reporting of apparent CIP violations can provide the FDIC greater assurance that institutions with weak programs for detecting money laundering and terrorist financing activity are identified and appropriate and timely corrective measures are taken.

Although not required by statute or regulation, BSA/AML risk assessments are emphasized in examination guidance to provide a means for (1) institutions to design risk-based BSA/AML compliance programs, which include internal controls, to mitigate risks and (2) examiners to scope and plan their evaluation of the adequacy of BSA/AML compliance programs. Concerning the risk assessments, we found that 21 of 24 sampled institutions had prepared the assessments. Examiners considered the institution-prepared risk assessments in BSA/AML examinations and took appropriate action in the three cases where institutions had not prepared assessments. Although the risk assessment is widely used in the design and examination of BSA/AML compliance programs, we noted that examiners were inconsistent in addressing and reporting on the risk categories and factors listed in the FFIEC BSA/AML Examination Manual. However, an Interagency Statement issued in July 2007 on enforcement of BSA/AML requirements specifically lists risk assessment as part of the system of internal controls mandated for institutions by regulation. This guidance should focus additional attention on the examination of risk assessments, including the use of designated risk categories and factors. Therefore, we are not making recommendations in this area at this time. Finally, we determined that risk assessments for 8 of the 24 financial institutions were based on a matrix format (Appendix J of the examination manual) intended for use by examiners that did not provide for a detailed assessment of risk categories and factors. Use of this matrix in lieu of a more thorough risk assessment could result in BSA/AML risks not being identified.

### Recommendations and Management Response

The report recommends that the Director, DSC (1) clarify guidance to examiners on the identification and reporting of apparent CIP violations and (2) provide instructions to examiners to clarify the circumstances under which Appendix J would be sufficient for use as a BSA/AML risk assessment. The FDIC's planned actions are responsive to our recommendations.



**DATE:** November 30, 2007

**MEMORANDUM TO:** Sandra L. Thompson, Director  
Division of Supervision and Consumer Protection

**FROM:** /Signed/  
Russell A. Rau  
Assistant Inspector General for Audits

**SUBJECT:** *FDIC's Implementation of the USA PATRIOT Act*  
(Report No. AUD-08-003)

This report presents the results of the subject FDIC Office of Inspector General (OIG) audit. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act)<sup>1</sup> was signed into law on October 26, 2001, as a response to the September 11, 2001 terrorist attacks. Title III of the Patriot Act—International Money Laundering<sup>2</sup> Abatement and Financial Anti-Terrorism Act of 2001<sup>3</sup>—is intended to facilitate the prevention, detection, and prosecution of international money laundering and terrorist financing and consists of provisions related to (1) international counter-money laundering and related measures, (2) Bank Secrecy Act<sup>4</sup> (BSA) amendments and related improvements that supplement U.S. authority provided under the BSA to detect money laundering, and (3) currency crimes and protection. The FDIC's Division of Supervision and Consumer Protection (DSC) monitors FDIC-supervised financial institutions' compliance with the Patriot Act Title III requirements.

The audit objectives were to determine whether (1) examination procedures are designed to evaluate institution compliance with the anti-money laundering (AML) and terrorist financing provisions of the Patriot Act and (2) those procedures were fully and consistently implemented to provide reasonable assurance that institutions with weak programs for detecting money laundering and terrorist financing activity will be identified and appropriate corrective measures taken. We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix I of this report discusses our objectives, scope, and methodology in detail.

---

<sup>1</sup> Public Law No. 107-56.

<sup>2</sup> Money laundering is the process by which criminals or criminal organizations seek to disguise the illicit nature of their proceeds by introducing them into the stream of legitimate commerce and finance.

<sup>3</sup> Title III of the Patriot Act includes 46 sections of which only 12 sections relate to financial institutions. Of those 12 sections, only 8 need examination procedures. There are nine additional titles of the Patriot Act that are not related to financial institutions or the FDIC's supervision and examination of financial institutions.

<sup>4</sup> Public Law No. 91-508, codified to 31 U.S. Code (U.S.C.), Section 5311 et seq.

## **BACKGROUND**

Emphasis on AML efforts, in general, and the international fight against money laundering and terrorist financing, in particular, has risen significantly since the September 11, 2001 terrorist attacks. The PATRIOT Act made a number of amendments to the AML provisions of the BSA, also known as the Currency and Foreign Transactions Reporting Act. Congress passed the BSA to (1) prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of, money derived from criminal activity and (2) help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions.

The BSA authorizes the Department of the Treasury (Treasury) to require financial institutions to establish BSA/AML compliance programs;<sup>5</sup> file certain reports that are used in criminal, tax, or regulatory investigations or proceedings; and keep certain records of transactions. The BSA's implementing regulation<sup>6</sup> is used to aid law enforcement agencies in the investigation of suspected criminal activity such as illegal drug activities, income tax evasion, and money laundering by organized crime. The PATRIOT Act expanded the Treasury's authority to regulate the activities of U.S. financial institutions, especially their relations with entities and individuals with foreign ties, and increased the focus on terrorist financing activities. The Financial Crimes Enforcement Network (FinCEN), a bureau of the Treasury, is the delegated administrator of the BSA. FinCEN issues regulations and interpretive guidance, provides outreach to regulated industries, and supports the examination function of the Federal Banking Agencies (FBA),<sup>7</sup> and pursues civil enforcement actions, when warranted.

### **Examination Procedures Related to AML and Terrorist Financing Provisions of the PATRIOT Act**

Although overall authority for BSA enforcement and compliance remains with the Treasury, its regulations delegate authority to the FBAs, including the FDIC, to examine financial institutions for compliance. In addition, Section 8(s) of the Federal Deposit Insurance (FDI) Act,<sup>8</sup> provides the FDIC authority to examine and enforce compliance at FDIC-supervised financial institutions. Since the PATRIOT Act amended the BSA, each BSA/AML examination also encompasses a

---

<sup>5</sup>The FDIC Rules and Regulations, Section 326.8, *Bank Secrecy Act Compliance*, and Treasury's implementing regulations for BSA/AML and PATRIOT Act compliance, 31 Code of Federal Regulations (C.F.R.) Part 103, require financial institutions to implement a BSA/AML compliance program that includes the minimum program requirements (referred to as "pillars"). The pillars include customer identification programs, systems of internal controls, independent testing, designated BSA compliance officers, and training for appropriate personnel.

<sup>6</sup> 31 C.F.R. Part 103.

<sup>7</sup> The FBAs are the Board of Governors of the Federal Reserve System, FDIC, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, which together form the Federal Financial Institutions Examination Council (FFIEC).

<sup>8</sup> Codified to 12 U.S.C. 1818(s). The FDI Act requires the FDIC to (1) prescribe regulations requiring financial institutions to establish and maintain procedures reasonably designed to ensure and monitor compliance; (2) review such procedures during their examinations of these institutions and report problems with compliance in reports of examination; and (3) enforce compliance with the BSA monetary transaction recordkeeping and reporting requirements, including issuance of Cease and Desist (C&D) orders for noncompliance.

review of financial institutions' compliance with PATRIOT Act requirements.<sup>9</sup> In June 2005, the FFIEC issued interagency guidance in the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual* (FFIEC BSA/AML Examination Manual or examination manual) to provide examination procedures related to BSA, AML, PATRIOT Act, and Office of Foreign Assets Control (OFAC)<sup>10</sup> compliance. The FFIEC members revised the FFIEC BSA/AML Examination Manual in July 2006<sup>11</sup> to update examination procedures related to BSA/AML and PATRIOT Act compliance. Table 1 outlines the specific sections of the PATRIOT Act for which the FDIC and other FBAs have issued examination guidance.

**Table 1: Status of Examination Procedures for PATRIOT Act Provisions**

PATRIOT Act Title III Section*	Examination Procedures Included in the FFIEC BSA/AML Examination Manual
Section 311-Special Measures for Financial Institutions	Yes
Section 312-Special Due Diligence	Yes
Section 313-Prohibition on U.S. Correspondent Accounts	Yes
Section 314-Cooperative Efforts to Deter Money Laundering (Information Sharing)	Yes
Section 319-Forfeiture of Funds	Yes
Section 325-Concentration Accounts at Financial Institutions	Yes
Section 326-Verification of Identification (Customer Identification Programs)	Yes
Section 352-Anti-Money Laundering Programs	Yes

Source: OIG review of the FFIEC BSA/AML Examination Manual, dated July 28, 2006.

\*Some of the names of the Title III sections have been abbreviated for the purposes of this table.

Appendix II provides additional information on the status of regulations and examination procedures for PATRIOT Act sections.

### **Supervisory and Enforcement Guidance Related to the Identification and Correction of BSA/AML Compliance Program Deficiencies**

Noncompliance with BSA/AML and PATRIOT Act requirements could expose financial institutions to actions from the FDIC and other FBAs, Treasury, and/or Department of Justice.

<sup>9</sup> DSC conducts BSA/AML examinations in conjunction with FDIC risk management examinations and those of state regulatory agencies that do not incorporate BSA/AML procedures into their examinations. According to DSC, as of May 14, 2007, six state regulatory agencies did not review BSA/AML compliance during their examinations.

<sup>10</sup> OFAC regulations prohibit financial institutions from engaging in transactions with the governments of, or individuals or entities associated with, foreign countries against which federal law imposes trade or economic sanctions. Sanctions also can be used against dangerous groups and individuals, such as international narcotics traffickers, terrorists, and foreign terrorist organizations, regardless of national affiliation.

<sup>11</sup> On August 2, 2006, the FDIC issued a Financial Institution Letter (FIL) to FDIC-supervised institutions, announcing the release of the revised FFIEC BSA/AML Examination Manual. The FIL acknowledged that the manual included (1) guidance on risk-based policies, procedures, and processes for banking organizations to comply with the BSA and safeguard operations from money laundering and terrorist financing and (2) enhanced guidance on the risk assessment process, including the development of BSA/AML risk assessments and examiner evaluation of those assessments. In addition to the 2006 revision, the FFIEC issued a revised BSA/AML Examination Manual on August 24, 2007. Significant updates to the 2007 examination manual include clarification on regulatory expectations between lower-risk and higher-risk customers for customer due diligence purposes.

Specifically, the FDIC can impose supervisory and/or enforcement actions and has issued guidance to its examiners that outlines its authority to impose such actions. For example, in October 2006, the FDIC issued a Regional Directors (RD) memorandum entitled, *Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements*. The memorandum provides specific guidance to assist examiners in determining when to recommend C&Ds for noncompliance with BSA/AML and PATRIOT Act requirements. In addition, on July 19, 2007, the *Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements* (Interagency Statement) was issued by the FBAs, establishing the agencies' policy on circumstances in which an agency will issue a C&D to address noncompliance with certain BSA/AML requirements. The FDIC transmitted the Interagency Statement to the institutions it supervises on August 23, 2007. In accordance with Section 8(s) of the FDI Act, the FDIC is authorized to issue a C&D if an institution has failed to establish and maintain a BSA compliance program or has failed to correct any previously reported problem with the program.

The FDIC has imposed actions to correct noncompliance with BSA and PATRIOT Act provisions, as indicated in Table 2. In addition, in compliance with an information-sharing Memorandum of Understanding<sup>12</sup> (MOU) between FinCEN and the FBAs, the FDIC has referred certain financial institutions to FinCEN for consideration of civil money penalties (CMP) for noncompliance with BSA provisions.

**Table 2: Supervisory and Enforcement Actions for Noncompliance with BSA/AML and PATRIOT Act Requirements**

<b>FDIC Supervisory and Enforcement Actions</b>	<b>Number of Actions Imposed</b>
Informal Supervisory Actions <sup>a</sup>	131
Formal Enforcement Actions <sup>b</sup>	11
Referrals Forwarded to FinCEN	22

Source: OIG review of FDIC Formal and Informal Action Tracking System data for the period September 1, 2005 through October 31, 2006; review of ROEs for sampled financial institutions; discussions with DSC officials; and review of referrals that DSC forwarded to FinCEN for the period September 1, 2005 through December 31, 2006.

<sup>a</sup> Informal supervisory actions include Memorandum of Understanding (MOU), Bank Board Resolution, and any other informal action taken by the FDIC.

<sup>b</sup> Formal enforcement actions include C&D, CMP, and any other formal action taken by the FDIC.

### **Customer Identification Programs**

Of the five BSA/AML compliance program pillars (see footnote 5), only the requirement for financial institutions to implement a Customer Identification Program (CIP) directly resulted from enactment of the PATRIOT Act. Specifically, Section 326 of the PATRIOT Act, which is implemented through Treasury regulations 31 C.F.R. Part 103.121 and Section 326.8 of the FDIC's Rules and Regulations, requires banks to implement a written, board-approved CIP that

<sup>12</sup> On September 30, 2004, the FBAs entered into an MOU with FinCEN to provide information related to BSA/AML examinations and enforcement actions and each FBA's BSA examination program. It is FDIC policy to refer significant BSA violations by FDIC-supervised institutions to FinCEN for review and possible assessment of civil and/or criminal penalties. Referrals to FinCEN should generally be considered when the types and nature of apparent violations of the BSA expose the institution to a heightened level of exposure to potential money laundering activity, demonstrate a willful or flagrant disregard of the requirements of the BSA, or result from nonexistent or seriously deficient BSA/AML compliance programs.

is appropriate for the institution's size and type of business. The CIP must include (1) account-opening<sup>13</sup> procedures that specify the identifying information that will be obtained from each customer,<sup>14</sup> and (2) reasonable and practical risk-based procedures for verifying the identity of each customer. These procedures must be based on the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank; the various methods of opening accounts provided by the bank; the various types of identifying information available; and the bank's size, location, and customer base. The FFIEC BSA/AML Examination Manual identifies an objective for examiners to assess a bank's compliance with the statutory and regulatory requirements for a CIP. Appendix III provides additional information on the requirements related to CIPs.

## **Risk Assessments**

Various sections of the PATRIOT Act, such as those addressing CIPs, correspondent accounts,<sup>15</sup> and concentration accounts,<sup>16</sup> address the linkage between risk and the establishment of appropriate controls within the BSA/AML compliance programs of financial institutions. These risks include terrorist financing, money laundering, and other criminal activity. One means by which institutions can gain an understanding of these risks is through development of a BSA/AML risk assessment. BSA/AML risk assessments are not specifically required by statute or regulation, but are set forth in the FFIEC BSA/AML Examination Manual as a good business practice for institutions to use in developing risk-based controls in their BSA/AML compliance programs and, therefore, also for compliance with the PATRIOT Act. In fact, in the 2006 version of the manual, risk assessment was given its own section to emphasize its importance in the design of effective controls at institutions and in the BSA/AML examination process. Figure 1, on the next page, shows how the financial institution's risk assessment links to the overall BSA/AML compliance program.

---

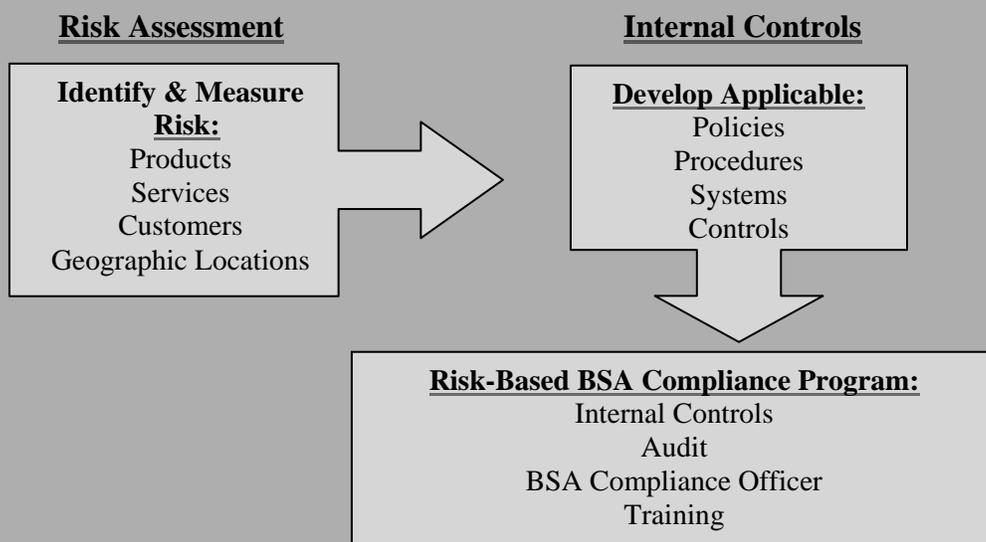
<sup>13</sup> For CIP purposes, an account is a formal banking relationship to provide or engage in services, dealings, or other financial transactions and includes a deposit account, a transaction or asset account, a credit account, or another extension of credit. An account also includes a relationship established to provide a safe deposit box or other safekeeping services or to provide cash management, custodian, or trust services.

<sup>14</sup> For CIP purposes, a customer is defined as a person (an individual, a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity, and an individual who opens a new account for an entity that is not a legal person. There are certain situations that can be excluded from the definition of customer for CIP purposes such as (1) a person who does not receive banking services, for example a person whose loan application is denied; or (2) an existing customer, as long as the bank has a reasonable belief that it knows the customer's true identity.

<sup>15</sup> A correspondent account is maintained by a bank with another bank for the deposit or placement of funds for themselves or their customers. Although these accounts may be developed and used primarily for legitimate purposes, international correspondent bank accounts may pose increased risk of illicit activities, including money laundering and terrorist financing.

<sup>16</sup> A concentration account is an internal account established by the bank to facilitate the processing and settlement of multiple or individual customer transactions within the bank, including a suspense, settlement, intra-day, sweep, or collection account.

**Figure 1: Risk Assessment Link to the BSA/AML Compliance Program**



Source: FFIEC BSA/AML Examination Manual, Appendix I.

According to the FFIEC BSA/AML Examination Manual, examiner scoping and planning for financial institution examinations generally begins with an analysis of the institution's BSA/AML risk assessment.<sup>17</sup> Examiners should determine whether the institution has adequately identified the risk associated with compliance with BSA/AML requirements and implementation of the PATRIOT Act in its banking operations which, as indicated above, include its products, services, customers, and geographic locations. Further, the July 2007 Interagency Statement lists risk assessment as part of the system of internal controls, which, like the CIP, is one of the five required pillars of a BSA/AML compliance program.

### **Additional Steps to Address PATRIOT Act Compliance**

In addition to issuing FILs to FDIC-supervised institutions to inform them of related examination and enforcement guidance, the FDIC has taken a number of steps to strengthen PATRIOT Act compliance. For example, the FDIC has:

- Conducted training and outreach sessions for its examiners and the banking industry, including providing presentations at various industry conferences and seminars targeting BSA/AML and counter-financing of terrorism issues. Training and outreach activities included discussions on the revisions to the 2006 FFIEC BSA/AML Examination Manual.

<sup>17</sup> In addition to reviewing the financial institution's BSA/AML risk assessment, during the scoping and planning process, examiners generally analyze prior examination reports and work papers; independent reviews or audit results; and other information, including but not limited to, training documentation, suspicious activity reporting data, and OFAC compliance information.

- Taken steps to ensure that examiners complete a mandatory training curriculum related to BSA/AML and the PATRIOT Act and certified a number of its BSA subject matter experts under the Association of Certified AML Specialists<sup>18</sup> certification program.
- Issued RD Memoranda, including the updated FDIC *Risk Management Manual of Examination Policies*; various fact sheets; and frequently asked questions on issues such as CIP and information sharing.<sup>19</sup>
- Revised BSA-related violation codes to specifically include PATRIOT Act requirements.
- Established performance measures that address BSA/AML and PATRIOT Act compliance.
- Created a National BSA/AML Task Force and participated in various BSA/AML and PATRIOT Act-related working groups to address BSA/AML policy and procedural matters. Under the auspices of the FFIEC BSA/AML Working Group, which was created in June 2004, the FBAs developed the interagency examination procedures in the FFIEC BSA/AML Examination Manual. In addition, the FDIC is a member of the BSA Advisory Group Examination Subcommittee, which meets with the banking industry to solicit feedback regarding money-laundering risks,<sup>20</sup> and works with the Conference of State Bank Supervisors (CSBS) on updates to BSA/AML examination guidance.<sup>21</sup>

## RESULTS OF AUDIT

The FDIC, in conjunction with the FFIEC, has issued comprehensive examination procedures in the FFIEC BSA/AML Examination Manual designed to assist examiners in evaluating institution compliance with the AML and terrorist financing provisions of the PATRIOT Act. Additionally, the FDIC has issued supervisory and enforcement guidance on corrective actions for noncompliance with the BSA and PATRIOT Act and referrals of significant BSA violations to FinCEN for review and possible assessment of civil and/or criminal penalties. Notably, the FDIC has taken formal and informal action in a number of cases to address noncompliance with BSA and PATRIOT Act provisions and related regulations and made referrals to FinCEN as required based on the information-sharing MOU with FinCEN. The FDIC has also taken steps to

---

<sup>18</sup> The Association of Certified Anti-Money Laundering Specialists is a membership-based organization that serves as a platform for career development and professional networking for individuals in the AML field. The organization provides resources for financial institutions and related businesses that help train, identify, and locate individuals who specialize in money-laundering control policies, procedures, and regulations.

<sup>19</sup> Information sharing relates to Section 314 of the PATRIOT Act (see Appendix II).

<sup>20</sup> The BSA Advisory Group was established on March 10, 1994 to give the Treasury advice on strengthening AML programs and simplifying currency reporting forms. The broad-based advisory group includes officials from federal and state government agencies, banking and other private-sector enterprises where money-laundering activities are sometimes attempted, and law enforcement. The Director of FinCEN serves as the chair of the group, which consists of 52 members; meets bi-annually; and includes subcommittees for issues, including, but not limited to, examinations, suspicious activity reporting, and privacy and security.

<sup>21</sup> CSBS provides insight into the state perspective on federal regulatory policy proposals that directly affect state-chartered banks and state bank supervisors. CSBS represents state supervisors on the working groups of the FFIEC and helps to coordinate issues for the state banking departments on supervisory-related issues.

strengthen BSA and PATRIOT Act compliance, including training and industry outreach, certifications for AML specialists, and the establishment of BSA-related performance measures.

Generally, FDIC examiners implemented examination procedures in the FFIEC BSA/AML Examination Manual related to the PATRIOT Act. However, the FDIC could enhance the implementation of examination procedures with respect to CIPs. The FDIC examiners reviewed CIPs for all 24 of our sampled financial institutions and cited CIP-related violations at 5 of those institutions. However, we found other apparent violations of CIP requirements that were not consistently identified and reported by examiners. The CIP requirements are intended to ensure that a financial institution can form a reasonable belief that it knows the true identity of its customers. Consistent examiner identification and reporting of apparent CIP violations can provide the FDIC greater assurance that institutions with weak programs for detecting money laundering and terrorist financing activity are identified and appropriate and timely corrective measures are taken (**Implementation of Examination Procedures for Customer Identification Programs**).

Although not specifically required by statute or regulation, BSA/AML risk assessments are emphasized in examination guidance to provide a means for (1) institutions to design risk-based BSA/AML compliance programs, which include internal controls, to mitigate risks and (2) examiners to scope and plan their evaluation of the adequacy of BSA/AML compliance programs. Concerning the risk assessments, we found that 21 of 24 sampled institutions had prepared the assessments. Examiners considered the institution-prepared risk assessments in BSA/AML examinations and took appropriate action in the 3 cases where institutions had not prepared assessments. While it is notable that risk assessment is widely used in the design and examination of BSA/AML compliance programs, we observed inconsistencies in addressing and reporting on the risk categories and factors listed in the FFIEC BSA/AML Examination Manual. However, the July 2007 Interagency Statement on enforcement of BSA/AML requirements specifically lists risk assessment as part of the system of internal controls mandated for institutions by regulation. The Interagency Statement should focus additional attention on the design and examination of risk assessments, including the use of designated risk categories and factors. Therefore, we are not making recommendations in this area at this time. Finally, we determined that risk assessments for 8 of the 24 financial institutions were based on a matrix format intended for use by examiners that did not provide for a detailed assessment of risk categories and factors. Use of this matrix in lieu of a more thorough risk assessment could result in BSA/AML risks not being identified (**Implementation of Examination Procedures for Risk Assessments**).

## **IMPLEMENTATION OF EXAMINATION PROCEDURES FOR CUSTOMER IDENTIFICATION PROGRAMS**

The FDIC could enhance the implementation of examination procedures in the FFIEC BSA/AML Examination Manual concerning institution CIPs. Although examiners reviewed CIPs for all of the 24 sampled financial institutions and cited CIP-related violations at 5 of those institutions, we found other apparent violations of CIP requirements in the programs that were not consistently identified and reported by examiners to the FDIC and to financial institution

management. The CIP requirements, such as having procedures to verify a customer's identity prior to opening an account, are intended to ensure that the financial institution can form a reasonable belief that it knows the true identity of its customers. Consistent examiner identification and reporting of apparent CIP violations can provide the FDIC greater assurance that institutions with weak programs for detecting money laundering and terrorist financing activity are identified and appropriate and timely corrective measures are taken.

## **Requirements Related to the CIP**

Section 326 of the USA PATRIOT Act<sup>22</sup> requires financial institutions to implement a written, board-approved CIP, appropriate for the institution's size and type of business, which includes, at a minimum, procedures for:

- verifying a customer's true identity to the extent reasonable and practicable and defining the methodologies to be used in the verification process,
- collecting specific identifying information from each customer when opening an account,
- responding to circumstances and defining actions to be taken when a customer's true identity cannot be appropriately verified with "reasonable belief,"
- maintaining appropriate records during the collection of information and verification of a customer's identity,
- verifying a customer's name against a federal government list of known or suspected terrorists or terrorist organizations,<sup>23</sup> and
- providing customers with adequate notice that the bank is requesting identification to verify their identities.

The FFIEC BSA/AML Examination Manual directs examiners to assess financial institution compliance with the statutory and regulatory requirements for CIPs. Examiners should verify whether a financial institution's policies, procedures, and processes include a comprehensive program to identify customers who open an account after October 1, 2003. The CIP must be examined as part of the institution's BSA/AML compliance program. Additionally, the manual states that examination findings should be discussed with the bank's management and all significant findings must be included in the ROE. In addition, the FDIC's *Risk Management Manual of Examination Policies* provides guidance to examiners related to the institution's written, board-approved CIP. The manual outlines specific requirements such as (1) account-opening procedures that specify the identifying information to be obtained from each customer, (2) procedures for verifying the information, and (3) record retention requirements.

## **Identification of Apparent Violations**

Our review of written institution CIP policies, examination workpapers, and ROEs for 24 sampled financial institutions indicated that the institutions' CIPs did not always address all CIP requirements necessary to verify the identity of customers who open new accounts with the institutions. We also found that examiners were not consistent in some cases in their

---

<sup>22</sup> Implemented by 31 C.F.R. 103.121.

<sup>23</sup> According to the FFIEC BSA/AML Examination Manual, there are no designated government lists against which banks could compare customer names specifically for CIP purposes.

identification of apparent violations of CIP requirements. For example, some financial institutions were cited for not including all required customer verification procedures in their CIPs, while others were cited only for apparent violations identified during transaction testing performed as part of the examination, even though the CIPs for those institutions were also found to not include all requirements. In fact, for the five financial institutions in our sample where CIP violations were cited, examiners' decisions to cite the institutions were generally based on the results of their transaction testing rather than a review of the CIP. Examiners told us that they do not report in the ROE those deficiencies identified solely in the CIP policies – rather, the examiners usually recommend orally or informally that bank management consider those deficiencies in updates to the CIP. Additionally, some examiners included recommendations in the ROEs related to complying with CIP requirements but did not cite violations. The inconsistencies in reporting could result in weak compliance programs remaining uncorrected for extended periods.

Based on our review of the examination workpapers and ROEs for the 24 sampled institutions, including copies of the institutions' CIP policies, we determined that:

- CIPs for the 5 institutions cited by DSC examiners for apparent CIP violations had other apparent CIP violations that were not cited in the ROE violations section,
- CIPs for the each of the remaining 19 financial institutions in our sample had at least 1 apparent CIP violation that was not cited, and
- 3 institutions could have been but were not cited for 5 or more apparent CIP violations.

Table 3, on the next page, provides a synopsis of CIP violations cited by examiners and some of the more frequent apparent CIP violations at the 24 sampled institutions that were not cited by the examiners.

**Table 3: Apparent CIP Violations**

<b>Violation Description</b> (Based on PATRIOT Act Section 326, Treasury 31 C.F.R. Section 103.121, and DSC violation descriptions)	<b>Number of Apparent CIP Violations</b>	
	<b>Apparent CIP Violations Cited by Examiners</b>	<b>Apparent CIP Violations not Cited by Examiners</b>
Failure of non-documentary procedures to address certain situations, such as where an individual is unable to present an unexpired government-issued identification document or where the customer opens an account without appearing in person.		15
Failure of CIP to include procedures when customer's identity is unknown and the financial institution cannot form a reasonable belief that it knows the true identify of a customer.		12
The CIP does not address when to obtain information about account control when an account is opened by a customer that is not an individual, and information about individuals with authority or control over such account, including signatories, is needed in order to verify the customer's identify.	1	10
Failure to implement a written CIP appropriate for its size and type of business.		6
Failure of CIP to contain procedures for verifying customer identity within a reasonable time after the account is opened.		3
Failure of CIP to contain procedures that describe nondocumentary methods used, including public databases, checking references with other financial institutions, and obtaining a financial statement.		3
Failure to keep minimum records required under Section 103.121 for a period of 5 years after the account is closed, including the customer's name; date of birth for individuals; address; and identification number.	4	3
Failure to obtain minimum information prior to account opening, such as the customer's name; date of birth for individuals; address; and identification number.	3	
Failure to properly address situations where the Tax Identification Number (TIN) is not obtained, including confirmation that an application for a TIN was filed before the customer opened the account and to obtain the TIN within a reasonable period of time after the account is opened.	1	
Failure to meet certain conditions if relying on another financial institution, such as an affiliate, to perform any procedures included in its CIP.	1	
Failure of CIP to specify which identifying information will be obtained from each customer to open an account.	1	

Source: OIG review of CIPs, examination work papers, and ROEs for sampled financial institutions.

In summary, although examiners cited some financial institutions for apparent CIP violations, all 24 of the financial institutions in our sample had apparent violations that were not cited in the ROEs. The need to cite apparent violations of CIP requirements when they occur was recently emphasized in the October 4, 2006 RD memorandum entitled, *Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements*, which states that apparent violations of individual pillars of the BSA/AML compliance program (CIP is one of the pillars) should be cited when detected. Importantly, supervisory actions were taken with regard to one of the five sampled institutions cited in the ROEs for apparent CIP violations but were not taken for the other four institutions. As established by Section 8(s)(3)(B) of the FDI Act<sup>24</sup> apparent violations that persist across multiple examinations are subject to a C&D to correct the underlying compliance problem at the institution. Therefore, it is important for examiners to cite CIP violations when detected.

## **Conclusion**

CIPs, which should be designed to ensure that financial institutions know the true identity of their customers, are required to be included in the institutions' overall BSA/AML compliance program and to address all of the program requirements specified by the PATRIOT Act and FDIC Rules and Regulations. An effective CIP helps to ensure that a financial institution knows the true identity of its customers and serves as a deterrent to criminal use of the nation's financial system. We consider the inconsistencies in the identification and reporting of apparent CIP violations to be indicative of the need for additional instruction to examiners regarding their review of CIPs. Consistent examiner identification and reporting of apparent CIP violations will provide DSC greater assurance that (1) FDIC-supervised financial institutions are complying with BSA and PATRIOT Act requirements and (2) institutions with weak programs for detecting money laundering and terrorist financing activity are identified and appropriate and timely corrective measures are taken.

DSC stated that, in determining whether there are apparent violations, examiners consider not only the institution's CIP policy but also any supplemental procedures and forms used by the institution to ensure BSA compliance. To the extent that these procedures or forms were in the institution's overall BSA policy, we included these documents in our review. However, these procedures and forms were not always included in the examination workpapers, so it is possible, based on this supplemental information, that certain deficiencies in institution CIP policies might not be considered apparent violations by the examiners. Also, some examiners informed us that they only cited apparent violations based on transaction testing, while other examiners cited apparent violations based on CIP policy deficiencies. Consequently, there appears to be a need for additional examination guidance addressing the consideration of supplemental procedures and forms in evaluating CIP policies and whether transaction testing is a necessary basis for citing apparent CIP violations.

---

<sup>24</sup> RD Memorandum entitled, *Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements*, dated October 4, 2006, provides guidance on actions that the FDIC is authorized to implement under Section 8(s)(3)(B) of the FDI Act.

## Recommendation

We recommend the Director, DSC:

1. Clarify guidance to examiners on the identification and reporting of apparent CIP violations, including the consideration of supplemental procedures and forms and whether transaction testing is a necessary basis for citing apparent CIP deficiencies, to ensure that financial institutions implement CIPs appropriate for their BSA risk profile.

## IMPLEMENTATION OF EXAMINATION PROCEDURES FOR RISK ASSESSMENTS

Although not specifically required by statute or regulation, BSA/AML risk assessments are emphasized in examination guidance to provide a means for (1) institutions to design risk-based BSA compliance programs, which include PATRIOT Act requirements, to mitigate risks and (2) examiners to scope and plan their evaluation of the adequacy of BSA/AML compliance programs. We found that 21 of 24 sampled institutions had prepared risk assessments, and examiners took appropriate action when the assessments were not prepared. While it is notable that risk assessment is widely used by institutions to design BSA/AML compliance programs, we observed inconsistencies in addressing and reporting on the risk categories and factors designated in the BSA/AML Examination Manual. In addition, we determined that risk assessments for 8 of the 24 financial institutions were based on a matrix format, which did not provide for full consideration of the designated risk categories and factors. Use of this matrix in lieu of a risk assessment could result in BSA/AML risks not being identified.

### Examination Guidance for Risk Assessments

In 2006, the FFIEC members revised the FFIEC BSA/AML Examination Manual to, among other things, add a separate section dedicated to the development and evaluation of financial institution risk assessments.<sup>25</sup> The guidance states that financial institutions should adequately assess and document the risk exposures of the institution by identifying specific products and services, customers and entities, and geographic locations unique to the institution. For example, institutions located in high-risk geographic areas, such as High Intensity Financial Crimes Areas (HIFCA)<sup>26</sup> or High Intensity Drug Trafficking Areas (HIDTA),<sup>27</sup> are normally viewed as having a higher risk of criminal activity. We noted that 20 of the 24 financial institutions included in our sample were located in these high-risk areas. However, geographic location alone does not

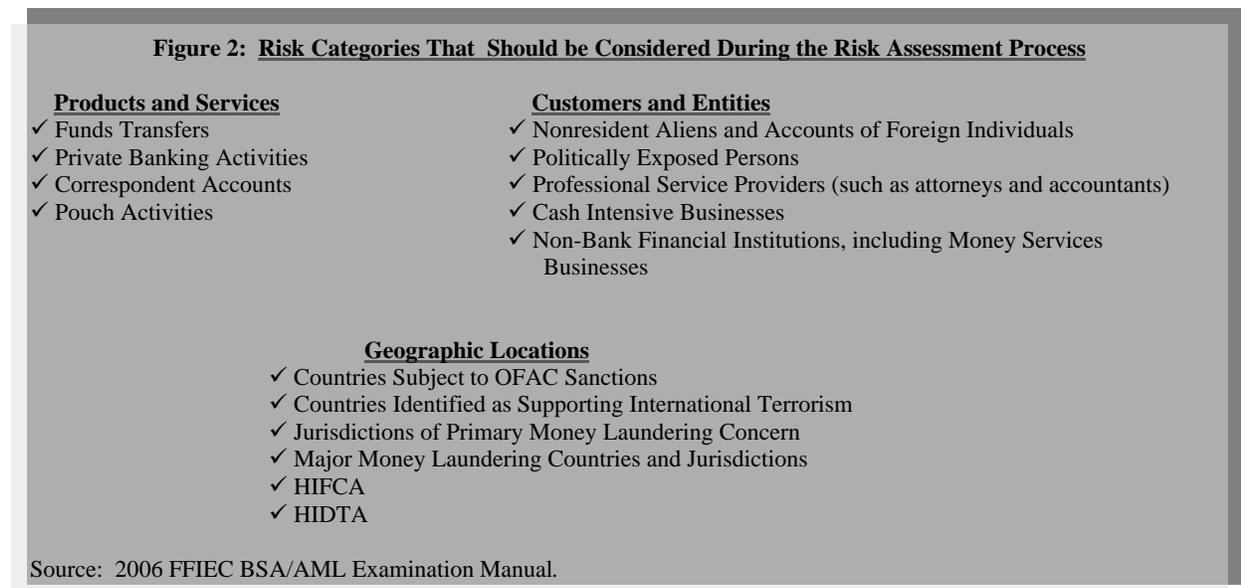
---

<sup>25</sup> The risk assessment section in the FFIEC BSA/AML Examination Manual was also added to promote consistency in this area, consolidate previous guidance on this topic, and provide additional instruction and support.

<sup>26</sup> HIFCAs, announced in the 1999 National Money Laundering Strategy, were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means to concentrate various levels of law enforcement (federal, state, and local) in high-intensity money laundering areas. Currently, there are seven regional HIFCA groups.

<sup>27</sup> The Anti-Drug Abuse Act of 1988 and the Office of National Drug Control Policy (ONDCP) Reauthorization Act of 1998 authorized the Director of ONDCP to designate areas within the United States that exhibit serious drug trafficking problems and harmfully impact other areas of the country as HIDTAs. The HIDTA Program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. Currently, there are 28 geographical areas designated as HIDTAs.

necessarily determine a customer's or transaction's risk level. Figure 2 provides additional details on the three risk categories.



The FFIEC BSA/AML Examination Manual also discusses five factors to be considered in its risk assessment process:

- purpose of the account,
- actual or anticipated activity,
- nature of the customer's business,
- customer's location, and
- types of products and services used by the customer.

The factors are applied as part of a detailed analysis of bank data—the risk assessment—to gain an understanding of the bank's risk profile, including the varying levels of risk associated with the institution's activities and customers. The examination manual states that a risk assessment should be used by the bank to design effective risk-based controls for inclusion in its BSA/AML compliance program. In this regard, the manual indicates that institutions are expected to address the varying levels of risk associated with the categories specified above to facilitate the design and implementation of effective and efficient controls to mitigate identified risks. In addition, the examination manual states that analysis of specific risk factors is important because within any type of product or category of customer, there will be account holders that pose varying levels of risk.

The manual also states that examiners should use a risk assessment to scope, plan, and conduct examinations for BSA and PATRIOT Act compliance and to make an ultimate decision on the adequacy of the overall BSA/AML compliance program. According to the manual, examiners should review the institution's risk assessment, if one exists; independent audit results, including results of an independent review of the bank's BSA/AML risk assessment; and prior examination

results in addition to other information. If a financial institution has not completed a risk assessment or the examiner concludes that the bank's risk assessment is inadequate, the manual states that the examiner must complete a risk assessment based on available information and use Appendix J of the examination manual for that purpose. Further, examiners should conduct transaction testing to evaluate the adequacy of the bank's compliance with regulatory requirements; determine the effectiveness of its policies, procedures, and processes; and evaluate suspicious activity. The manual states that transaction testing is an important factor in forming conclusions about the integrity of the bank's overall controls and risk management processes.

The manual further states that examiners should evaluate the adequacy of an institution's BSA/AML risk assessment process. Examiners should also determine whether:

- the BSA/AML compliance program is effectively monitored and supervised in relation to the bank's risk profile as determined by the risk assessment and ascertain whether the BSA/AML compliance program is effectively mitigating the bank's overall risk;
- internal controls ensure compliance with the BSA and provide sufficient risk management, especially for high-risk operations (considering products, services, customers, and geographic locations);
- bank management's lack, or inaccurate assessment, of the bank's BSA/AML risks could be the underlying cause of policy, procedure, or process deficiencies; and
- there is a need for corrective actions, including the possibility of requiring the financial institution to conduct more detailed risk assessments.

### **Institution Preparation and Examiner Evaluations of Risk Assessments**

For the 24 sampled institutions, we determined that 3 institutions had not prepared risk assessments. In these cases, examiners took appropriate action.<sup>28</sup> Concerning the remaining 21 sampled institutions, FDIC examiners considered the institution-prepared risk assessment in BSA/AML examinations. However, we noted the following inconsistencies in the design of the institutions' risk assessments and related examinations by the FDIC.

- Seven financial institutions had prepared BSA/AML risk assessments that included comprehensive analyses of each of the risk categories and factors in the FFIEC BSA/AML Examination Manual and specified associated risk levels. However, risk

---

<sup>28</sup> For two of the three institutions without risk assessments, examiners completed a risk matrix—Appendix J—in accordance with the guidance in the FFIEC BSA/AML Examination Manual. For the third institution, the examiner concluded that the bank had not risk-rated its customer base, including money services businesses, embassy personnel, politically exposed persons, nonresident alien off-shore accounts, and foreign corporations. The bank also had not established and fully implemented risk-based customer due diligence or an adequate suspicious activity monitoring system, nor had the bank's independent audit addressed these areas or the absence of a BSA/AML risk assessment. The examiner cited the bank for violations related to internal controls. Although neither the bank nor the examiner had completed a risk assessment in this case, the examiner took a positive step and recommended an MOU that included provisions related to risk assessment, customer due diligence, and suspicious activity monitoring.

assessments for 14 institutions did not address at least one of the risk categories and factors and/or did not specify an associated risk level.

- Twelve examinations documented an overall conclusion on the adequacy of the risk assessment. In the remaining nine examinations, there was no apparent conclusion.
- Seven institutions had at least two consecutive examinations that identified deficiencies related to the institutions' risk assessments. However, internal control violations were cited in only four of these seven cases.

It is notable that institutions are generally using BSA/AML risk assessments as a component in the design and implementation of their compliance programs. As indicated above, 21 of 24 institutions had prepared risk assessments, and examiners documented conclusions on the adequacy of 12 of 21 assessments prepared by the institutions. Consistent examiner consideration and reporting on risk categories and factors listed in the FFIEC BSA/AML Examination Manual can provide the FDIC greater assurance that financial institutions identify BSA/AML-related risks and design effective risk-based controls necessary to mitigate those risks.

The Interagency Statement, issued on July 19, 2007, lists risk assessments as part of the system of internal controls for purposes of issuing C&Ds. This guidance has the potential to address the inconsistencies we noted in the design and examination of financial institution risk assessments. Specifically, the fact that risk assessment is now linked directly to the internal control pillar of the required BSA/AML compliance program focuses institution attention on preparing comprehensive risk assessments. In addition, directly linking the risk assessment to the internal control pillar should focus the examiner's attention on the importance of concluding on the adequacy of risk assessments and the citing of violations, where appropriate. Therefore, we are not making recommendations to address this matter at this time.

### **Use of Appendix J in the FFIEC BSA/AML Examination Manual for Assessing Risk**

When an institution has not completed or has an inadequate risk assessment, the FDIC expects examiners to obtain a general understanding of a bank's products and services, customers and entities, and geographic locations. The FFIEC BSA/AML Examination Manual instructs examiners to use Appendix J of the manual for this purpose. Because the risk assessment process should be comprehensive, it is understandable that examiners cannot conduct a detailed analysis of financial institution risks and that the high-level profile provided by Appendix J is appropriate for their use. In two cases, we noted that examiners used Appendix J because the BSA/AML risk assessment had not been completed by the institution.

However, financial institution use of Appendix J does not provide for detailed analysis of data related to five of the eight risk categories and factors that are part of the risk assessment process and evaluation of the bank's activities. According to the FFIEC BSA/AML Examination Manual, the complete analysis gives bank management a better understanding of the institution's risk profile in order to develop the appropriate policies, procedures, and processes to mitigate the

overall risk. Specifically, Appendix J does not include a detailed analysis of data for the following five factors:

- purpose of the account,
- actual or anticipated activity in the account,
- nature of the customer's business,
- customer's location, and
- types of products and services used by the customer.

The detailed analysis of the above five risk factors is important because, as stated in the FFIEC BSA/AML Examination Manual, within any type of product or category of customer, there will be accountholders that pose varying levels of risk.

We determined that 8 of the 24 financial institutions had used Appendix J, or a modified version of Appendix J, for their risk assessments. Although the manual recognizes that there are many formats that banks may use to effectively document a risk assessment, Appendix J, which is provided for examiner use—not institution use—did not provide for a detailed assessment of the risk factors listed above. The inclusion of Appendix J in the manual may give the impression to financial institutions that this format is acceptable and covers all risk categories and factors that should be assessed by institutions. Therefore, DSC should propose changes to Appendix J to clarify that it is not intended to be used by financial institutions in lieu of performing a comprehensive BSA/AML risk assessment.

DSC management indicated to us, during a discussion of our audit results, that institutions are not required to conduct BSA/AML risk assessments, although most institutions do so as a good management practice. DSC management also stated that there may be low-risk institutions for which examiners conclude that Appendix J provides a sufficient risk assessment. However, we found no criteria governing the definition of a low-risk institution or the use of Appendix J in lieu of a more comprehensive risk assessment. For example, in one case, we found that a large, complex institution with elevated BSA/AML risk used Appendix J for its risk assessment. Instructions to examiners would be beneficial to clarify the circumstances under which Appendix J would be sufficient for institution risk assessments.

## **Recommendation**

We recommend the Director, DSC:

2. Provide instructions to examiners to clarify the circumstances under which Appendix J would be sufficient for use as a BSA/AML risk assessment.

## **CORPORATION COMMENTS AND OIG EVALUATION**

On November 20, 2007, the Director, DSC provided a written response to a draft of this report. DSC's response is presented in its entirety as Appendix IV to this report. Regarding recommendations 1 and 2, by March 30, 2008, DSC will remind examination staff of supervisory

expectations and the appropriate utilization of guidance regarding the identification and reporting of apparent CIP violations and use of Appendix J.

DSC's actions are responsive to our recommendations. A summary of management's response to the recommendations is in Appendix V. The recommendations are resolved but will remain open until we have determined that agreed-to corrective actions have been completed and are effective.

## OBJECTIVES, SCOPE, AND METHODOLOGY

### Objectives

The objectives of this audit were to determine whether (1) examination procedures are designed to evaluate institution compliance with the AML and terrorist financing provisions of the PATRIOT Act and (2) those procedures were fully and consistently implemented to provide reasonable assurance that institutions with weak programs for detecting money laundering and terrorist financing activity will be identified and appropriate corrective measures taken. 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, 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. We performed our audit from September 2006 through May 2007.

### Scope and Methodology

To achieve our audit objectives, we:

- Obtained an understanding of FDIC and FFIEC guidance related to examination procedures for determining PATRIOT Act and BSA compliance by reviewing appropriate examiner and financial institution guidance.
- Interviewed DSC officials in Washington, D.C., and selected field offices and representatives of the FDIC's Legal Division in Washington, D.C.
- Identified and reviewed applicable criteria, including laws, rules, and regulations; examination guidance; and authorities related to examination and enforcement of BSA and PATRIOT Act compliance and the citing and tracking of violations related to compliance.
- Reviewed the following:
  - *Federal Register* notices and other agency and regulatory reports and related documents to gain an understanding of the FBAs' roles and responsibilities in implementing the PATRIOT Act.
  - The Treasury's Web site, including FinCEN's Web site, to obtain background information on the BSA and PATRIOT Act and to determine the status of the Treasury's rulemaking (proposed, interim, and final rules) related to the PATRIOT Act.
  - Related audit reports issued by the FDIC OIG and GAO.

To address our objective related to whether examination procedures were fully and consistently implemented, we limited our review to CIP and risk assessment-related procedures. In addition, we obtained information from DSC on examinations conducted after the release of the FFIEC BSA/AML Examination Manual, issued June 2005, and the updated manual issued July 28, 2006. We limited the sample universe to examinations completed September 1, 2005 to October 31, 2006. From those examinations, we selected a non-statistical sample of examinations for 24 FDIC-supervised financial institutions for detailed review.<sup>29</sup> To select the sample for review, we considered:

- size and geographic location of the financial institution and
- whether examiners had cited the financial institutions for PATRIOT Act violations.

For the sampled examinations, we reviewed ROEs, supporting work papers, correspondence files, supervisory and enforcement action information, and other pertinent documentation. We selected the sampled examinations from DSC's Atlanta, Kansas City, New York, and San Francisco regional offices. Additionally, we reviewed system data related to BSA examinations from DSC's Virtual Supervisory Information on the Net (ViSION), the automated system used by DSC to capture data on the results of DSC's reports of examination, including identified BSA violations. In addition, we reviewed system data from the Formal and Informal Action Tracking System, which captures information on supervisory and enforcement actions, and referrals that the FDIC forwarded to FinCEN in compliance with the 2004 information-sharing MOU between the FDIC, the other FBAs, and FinCEN.

Additionally, we coordinated with the IG Counsel, Office of Investigations, and other Office of Audits Directorates and FDIC Office of the Ombudsman.

### **Internal Controls**

We gained an understanding of the internal control activities relevant to the FDIC's examination process for BSA and PATRIOT Act compliance by identifying and reviewing applicable policies and procedures related to the FDIC's examinations for BSA and PATRIOT Act compliance, including guidance provided to FDIC examiners (FFIEC BSA/AML Examination Manual, FDIC *Risk Management of Examination Policies*, FILs, and Treasury regulations). Additionally, we interviewed DSC officials in the Washington, D.C., office; DSC representatives in selected regional and field offices; and the Examiners-in-Charge for the 24 sampled examinations.

Our assessment of internal controls determined that the FDIC has implemented some internal controls and examination guidance, including interagency examination procedures, related to examinations of financial institution compliance with the PATRIOT Act. However, controls related to the implementation of PATRIOT Act compliance programs need improvement, as indicated in our Results of Audit.

---

<sup>29</sup> The results of a non-statistical sample cannot be projected to the intended population by standard statistical methods.

## **Reliance on Computer-Based Data**

We used computer-based data and reports that DSC provided from the ViSION system to identify the universe of examinations conducted from September 1, 2005 through October 31, 2006. Although our audit identified certain inaccuracies in the ViSION data related to BSA and PATRIOT Act compliance, the data obtained from ViSION were not significant to our conclusions or recommendations. We also used information obtained from the FDIC's Formal and Informal Action Tracking System to identify supervisory and enforcement actions related to BSA/AML and PATRIOT Act compliance.

## **Compliance With Laws and Regulations, Government Performance and Results Act, and Fraud or Illegal Acts**

**Compliance with Laws and Regulations.** We reviewed applicable laws and regulations on PATRIOT Act compliance. We determined that the FDIC has general laws and regulations that relate to its overall examination authority (Section 10(b) of the FDI Act and Section 337.12 of the FDIC Rules and Regulations). The FDIC can rely on its general authority to impose enforcement actions under Section 8 of the FDI Act as it relates to operating a financial institution in an unsafe and unsound manner or noncompliance with laws and regulations to take action for PATRIOT Act compliance. The FDIC also has specific authority as outlined in Section 8(s) of the FDI Act as it relates to compliance with the BSA.

**Government Performance and Results Act.** We reviewed the *FDIC 2005-2010 Strategic Plan*, the *2006 Annual Performance Plan*, and DSC's divisional performance objectives to determine whether the Corporation and/or DSC had performance goals, objectives, and indicators or targets that specifically relate to the examination and enforcement of PATRIOT Act compliance or whether PATRIOT Act issues were generally included in matters related to BSA examination and compliance.

According to the *FDIC 2006 Annual Performance Plan*, the FDIC has established the following strategic goal, objective, and annual performance goals (see Table 4, on the next page) related to the risk management component of the FDIC's Supervision Program and to the supervision of financial institutions for compliance with the BSA/AML and PATRIOT Act.

**Table 4: The FDIC’s Activities to Address the Government Performance and Results Act**

Strategic Goal	Strategic Objective	Annual Performance Goals
FDIC-supervised institutions are safe and sound.	FDIC-supervised institutions appropriately manage risk.	Conduct on-site risk management examinations to assess the overall financial condition, management practices and policies, and compliance with applicable laws and regulations of FDIC-supervised depository institutions.
		Take prompt and effective supervisory action to address issues identified during the FDIC examination of FDIC-supervised institutions that receive a composite Uniform Financial Institutions Rating of “4” or “5” (problem institution). Monitor FDIC-supervised insured depository institutions’ compliance with formal and informal enforcement actions.
		Increase regulatory knowledge to keep abreast of current issues related to money laundering and terrorist financing.

Source: FDIC’s 2006 Annual Performance Plan.

The FDIC performs risk management examinations that include BSA examinations. Because the PATRIOT Act amended the BSA, an examination for PATRIOT Act compliance is included in BSA examinations. BSA compliance is a factor in assessing the willingness and ability of management to mitigate the operational risks of the bank and compliance with governing laws and regulations, which are a significant factor in the overall assessment of the condition of the institution.

In addition, according to the *2006 Annual Performance Plan*, the FDIC’s supervision program promotes the safety and soundness of FDIC-supervised insured depository institutions, protects consumers’ rights, and promotes community investment initiatives by FDIC-supervised insured depository institutions. As the primary federal regulator of all insured state non-member banks, the FDIC performs periodic examinations of those FDIC-supervised insured depository institutions to assess their overall financial condition, management policies and practices, and compliance with applicable laws and regulations.

In addition to FDIC corporate objectives, DSC has implemented a performance objective to assist in protecting the infrastructure of the U.S. banking system against terrorist financing, money laundering, and other financial crimes by implementing a comprehensive industry outreach and education effort on the BSA, AML, and counter-financing of terrorism issues.

**Fraud and Illegal Acts.** The nature of the audit objective did not require that we assess the possibility for fraud and illegal acts. However, during the audit, we were alert to the possibility of fraud and illegal acts, and no instances came to our attention.

### Prior Coverage

The FDIC OIG and the Government Accountability Office (GAO) have issued audit reports that relate to examination and enforcement of compliance with Title III of the PATRIOT Act. Table 5, on the next page, provides a synopsis of the prior FDIC audit coverage related to BSA compliance.

**Table 5: Synopsis of FDIC OIG Prior Audit Coverage of BSA and PATRIOT Act Compliance**

<b><i>FDIC's Supervision of a Financial Institution's Compliance With the Bank Secrecy Act</i></b> (Report No. 05-008), March 2005	
Audit Objective	To determine whether the FDIC adequately fulfilled its responsibilities to monitor and assure a financial institution's compliance with the BSA. We reviewed the (1) circumstances regarding the management of bank assets acquired from the FDIC, (2) adequacy of the FDIC's supervisory actions at the acquiring institution, and (3) FDIC's process for reporting BSA violations to the Treasury and law enforcement agencies.
Audit Results	The audit concluded that responsibilities to ensure compliance with the BSA were not adequately fulfilled by either institution management or the FDIC. Corporate governance at the financial institution and two former institutions was not sufficient to ensure that they met BSA requirements. The FDIC's examinations identified significant BSA violations and deficiencies, but the examinations generally lacked sufficient follow-up on corrective measures promised, but not implemented, by institution management. Consequently, weak BSA compliance programs persisted for extended periods. In addition, the FDIC should have more thoroughly considered the impact of BSA compliance violation and deficiency histories in connection with the Corporation's decision to qualify the potential acquirers of a failed institution.
<b><i>Supervisory Actions Taken for Bank Secrecy Act Violations</i></b> (Report No. 04-017), March 31, 2004	
Audit Objective	To determine whether DSC adequately followed up on BSA violations reported in examinations of FDIC-supervised financial institutions to ensure that they take appropriate corrective action. We specifically reviewed the FDIC's process for follow-up and other supervisory actions and the process and procedures for describing deficiencies and citing violations related to BSA noncompliance.
Audit Results	The audit identified several areas in which the FDIC needed to strengthen its supervisory oversight for BSA violations. Further, the report noted inconsistencies in describing BSA compliance program deficiencies and citing financial institutions for noncompliance. In addition, the FDIC's supervisory actions had not ensured to the greatest extent possible that institutions were in compliance with both the Treasury's and the FDIC's AML requirements. The FDIC needed to strengthen its follow-up process for BSA violations and had initiatives underway to reassess and update its BSA policies and procedures.
<b><i>The FDIC's Implementation of the USA PATRIOT Act</i></b> (Report No. 03-037), September 5, 2003	
Audit Objective	To determine whether the FDIC had developed and implemented adequate procedures to examine financial institutions' compliance with the PATRIOT Act.
Audit Results	The audit concluded that the FDIC's BSA examination procedures either partially or fully covered six of the eight applicable AML provisions contained in Title III of the PATRIOT Act and, therefore, did not cover two of the areas. With respect to those Title III provisions that required new or revised examination procedures, DSC was in the process of coordinating its efforts with other regulatory agencies and was drafting new or revised examination procedures to implement the provisions. However, DSC had not issued any new or revised examination procedures because it was either waiting for the Treasury to issue final rules implementing Title III provisions or coordinating the issuance of uniform procedures with an interagency steering committee.
<b><i>Examiner Assessment of Bank Secrecy Act Compliance</i></b> (Report No. 01-013), March 30, 2001	
Audit Objective	To determine the extent to which FDIC safety and soundness examinations reviewed institutions' compliance with the BSA.
Audit Results	The OIG recommended improvements in the FDIC's documentation of work related to the BSA.

Source: OIG synopsis of FDIC OIG reports related to BSA and PATRIOT Act compliance.

The GAO has also conducted audits related to PATRIOT Act compliance as indicated below.

***Opportunities Exist for FinCEN and the Banking Regulators to Further Strengthen the Framework for Consistent BSA Oversight***, GAO-06-386, dated April 2006.

The audit objective was to determine how (1) federal banking regulators examine for BSA compliance and identify and track violations to ensure timely corrective action and (2) enforcement actions are taken for violations of the BSA. The audit recognized the actions that the FDIC and other FBAs, along with FinCEN, have taken to strengthen the framework for BSA compliance, including more consistent examination procedures, recent improvements to automated tracking systems used to monitor BSA compliance, and efforts to share BSA-related information under an information-sharing MOU with FinCEN. However, the report recommended that FBAs and FinCEN:

- communicate emerging risks through updates of the interagency examination manual and other guidance;
- periodically review BSA violation data to determine if additional guidance is needed; and
- jointly assess the feasibility of developing a uniform classification system for BSA compliance problems.

FinCEN and the FBAs supported GAO's recommendations and expressed commitment to ongoing interagency coordination to address them.

***USA PATRIOT Act Additional Guidance Could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Procedures***, GAO-05-412, dated May 2005. The audit focused on Sections 326 and 314 of Title III of the PATRIOT Act. The audit objective was to determine how:

- the government “developed the regulations, educated the financial industry on them, and challenges it encountered”;
- regulators have updated guidance, trained examiners, and examined firms for compliance; and
- the new regulations have affected law enforcement investigations.

The GAO reported, in part, that although the FDIC and other FBAs have issued examination guidance related to Section 326 of the PATRIOT Act, examinations did not always determine whether financial institutions had adequately developed a CIP appropriate for their business lines and types of customers. The GAO also reported that this aspect of CIP is critical for ensuring that the identification and verification procedures are appropriate for the types of customers and accounts that are at higher risk of being linked to money laundering and terrorist activities. In addition, the GAO reported that some examinations also revealed implementation difficulties related to CIP that could lead to inconsistencies in the way examiners conduct examinations.

The GAO concluded that examiners and financial institutions may not always understand the requirement for a comparison of customer names against any list of known or suspected terrorists or terrorist organizations.

The GAO recommended that:

- the Treasury, through FinCEN, and with the federal financial regulators and state regulatory agencies, develop additional guidance on ongoing implementation issues.
- FinCEN work with the federal financial regulators to develop additional guidance for examiners to improve examinations of compliance with CIP requirements.

## STATUS OF REGULATIONS AND EXAMINATION PROCEDURES FOR PATRIOT ACT REQUIREMENTS

Title III Section <sup>a</sup>	PATRIOT Act Amendments to BSA	Final Rule Effective Date	Procedures included in <i>FFIEC BSA/AML Examination Manual</i> , issued July 2006
Section 311-Special Measures for Financial Institutions	Allows the Treasury to impose special measures related to foreign jurisdictions, financial institutions, and other accounts identified as primary money-laundering concerns.	Various <sup>b</sup>	Yes
Section 312-Special Due Diligence	Requires financial institutions that provide private banking accounts or correspondent accounts for foreign persons to establish enhanced due diligence procedures for those accounts. The section also requires enhanced due diligence for certain correspondent and private banking accounts. The effective date for compliance with the rule for new correspondent and private banking accounts was July 5, 2006 and October 1, 2006 for <u>existing</u> correspondent and private banking accounts.	July 5, 2006	Yes
Section 313-Prohibition on U.S. Correspondent Accounts <sup>c</sup>	Prohibits certain financial institutions from providing correspondent accounts to foreign banks with no physical presence in any country.	December 24, 2002	Yes
Section 314-Cooperative Efforts to Deter Money Laundering <sup>d</sup>	Requires the Treasury to issue regulations to encourage financial regulators and law enforcement officials to share information with financial institutions regarding persons reasonably suspected of engaging in terrorist acts or money laundering activities.	September 26, 2002	Yes
Section 319-Forfeiture of Funds <sup>c</sup>	Requires certain financial institutions that maintain correspondent accounts for foreign banks to maintain records regarding foreign banks.	December 24, 2002	Yes
Section 325-Concentration Accounts at Financial Institutions	Authorizes the Treasury to issue regulations concerning the maintenance of concentration accounts by financial institutions.	Final rule has not been issued <sup>e</sup>	Yes
Section 326-Verification of Identification	Amended the BSA to require that Treasury prescribe regulations to set minimum standards for identifying customers seeking to open accounts at financial institutions.	June 9, 2003 with an implementation date of October 1, 2003	Yes

**APPENDIX II**

<b>Title III Section<sup>a</sup></b>	<b>PATRIOT Act Amendments to BSA</b>	<b>Final Rule Effective Date</b>	<b>Procedures included in <i>FFIEC BSA/AML Examination Manual</i>, issued <b>July 2006</b></b>
Section 352-Anti-Money Laundering Programs <sup>f</sup>	Requires financial institutions to establish anti-money laundering programs and authorizes the Treasury to issue regulations for minimum standards. Under existing provisions of the BSA and Section 8 of the FDI Act, insured depository institutions are already directed to have such programs. Therefore, financial institutions that have established a BSA compliance program are already in compliance with the AML requirements under the PATRIOT Act. In an interim final rule, effective November 6, 2002, Treasury extended the applicability date for other financial institutions such as pawnbrokers, insurance companies, and travel agencies.	April 24, 2002 interim final rule	Yes

Source: OIG review of the FFIEC BSA/AML Examination Manual, dated July 28, 2006; PATRIOT Act Title III requirements; and *Federal Register* notices.

<sup>a</sup> Some of the names of Title III sections have been abbreviated for the purposes of this table.

<sup>b</sup> Treasury issues a final rule for each of the countries, entities, financial institutions, or foreign jurisdictions designated as a “primary money-laundering concern.”

<sup>c</sup> Sections 313 and 319 are usually referred to and discussed together because both sections amend 31 U.S.C. §5318.

<sup>d</sup> Cooperative Efforts to Deter Money Laundering is also referred to as Information Sharing.

<sup>e</sup> According to the FDIC, after the passage of the PATRIOT Act, the Treasury convened a working group for Section 325, but no rulemaking proposal for this section has yet been issued.

<sup>f</sup> The FDIC had already established applicable examination procedures before passage of the PATRIOT Act.

## CUSTOMER IDENTIFICATION PROGRAM REQUIREMENTS

The final rule for Section 326 of the PATRIOT Act, which became effective on June 9, 2003, provides a framework that includes the minimum standards that financial institutions must consider when identifying customers. Banks should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider the types of accounts offered; methods of opening accounts; types of identifying information available; and the bank's size, location, and customer base. The rule allows banks to develop a CIP tailored to the risk profile of the bank and impose risk-based procedures.

According to the FFIEC BSA/AML Examination Manual, a financial institution's CIP must include procedures:

- specifying information that will be obtained from each customer when accounts are opened;
- verifying the identity of the customer within a reasonable period of time after the account is opened based on the financial institution's risk;
- providing customers with adequate notice that the bank is requesting information to verify their identities;
- describing when it will use documents, nondocumentary methods, or a combination of both to verify identity;
- specifying the minimum acceptable documentation when a bank uses documentation methods to verify a customer's identity;
- outlining methods to be used when banks use nondocumentary methods to verify a customer's identity;
- addressing situations where, based on its risk assessment of a new account opened by a customer who is not an individual, the bank will obtain information about individuals with authority or control over such accounts, including signatories;
- determining whether the customer appears on any federal government list of known or suspected terrorists or terrorist organizations;<sup>30</sup> and
- addressing recordkeeping and retention of identifying information for a period of 5 years after the account is closed (for credit cards, the retention period is 5 years after the account is closed or becomes dormant).

---

<sup>30</sup> According to the FFIEC BSA/AML Examination Manual, there are no designated government lists specifically for CIP purposes. Customer comparisons to lists required by the OFAC and information sharing between federal law enforcement agencies and financial institutions, as outlined in 31 C.F.R. 103.100 of the Treasury's financial recordkeeping and reporting requirements, remain separate and distinct.

In addition, procedures should address circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. A financial institution is allowed to reasonably rely on another financial institution to perform its CIP procedures when certain conditions are met, including when the other institution is supervised by a federal financial regulator and establishes a contractual arrangement for annual certification that the institution has implemented an AML program.

The FDIC expanded Section 326.8 of its rules and regulations to require each FDIC-supervised institution to implement a CIP that complies with 31 C.F.R. 103.121 and incorporate the CIP into a bank's written, board-approved BSA compliance program (with evidence of such approval noted in the board meeting minutes). The *National Commission on Terrorist Attacks Upon the U.S.* and *Monograph on Terrorist Financing*<sup>31</sup> stressed the importance of Section 326 of the PATRIOT Act and recognized that effective customer identification may deter the use of financial institutions by money launderers and terrorists.

---

<sup>31</sup> The *9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the U.S.* and the accompanying *Monograph on Terrorist Financing* included information on combating terrorist financing and the role of financial institutions in the United States, including the terrorists' use of financial institutions in the planning and financing of those attacks.

## CORPORATION COMMENTS



**Federal Deposit Insurance Corporation**  
550 17th Street NW, Washington, D.C. 20429-9990

Division of Supervision and Consumer Protection

November 20, 2007

**TO:** Russell A. Rau  
Assistant Inspector General for Audits

**FROM:** Sandra L. Thompson [Signed]  
Director

**SUBJECT:** Response to Draft Report Entitled:  
*FDIC's Implementation of the USA PATRIOT Act (Assignment No. 2006-038)*

The Division of Supervision and Consumer Protection (DSC) appreciates that you found that in conjunction with the Federal Financial Institutions Examinations Council (FFIEC) we have issued comprehensive examination procedures. Further you note in your report "the FDIC has taken numerous steps to strengthen BSA and PATRIOT Act compliance, including training and industry outreach, certification for AML specialists, and establishment of BSA-related performance measures." We have evaluated your draft report and its emphasis on financial institution's Customer Identification Programs (CIP) and we provide the following comments regarding your recommendations.

**Inspector General Recommendations:**

We recommend the Director, DSC:

1. Clarify guidance to examiners on the identification and reporting of apparent CIP violations, including the consideration of supplemental procedures and forms and whether transaction testing is a necessary basis for citing apparent CIP deficiencies, to ensure that financial institutions implement CIPs appropriate for their BSA risk profile.

**DSC Response:**

As noted in your report, compliance with the CIP requires a variety of procedures which banks capture in numerous ways. This information may be in the actual BSA/CIP policy, in procedures retained by specific business line personnel and embedded within the forms to collect and verify CIP information. BSA examination procedures in the FFIEC BSA/AML Examination Manual require examination staff to verify the bank's comprehensive CIP procedures. Examiners identify where these procedures are maintained and only cite a violation if the procedures do not exist. Based upon these interagency examination steps, we do not believe that the additional technical record keeping requirements you reference are apparent violations. It was noted that no CIP program violations were identified in your sample.

**DSC Action:**

DSC will remind examination staff of supervisory expectations and the appropriate utilization of guidance by March 30, 2008.

2. Provide instructions to examiners to clarify the circumstances under which Appendix J would be sufficient for use as a BSA/AML risk assessment.

**DSC Response:**

The risk assessment is addressed in the FFIEC BSA/AML Examination Manual. We have considered your recommendation and in comparison to our supervisory experience we have determined that outstanding guidance is sufficient and can be further supported through a reminder to our examiners.

**DSC Action:**

DSC will remind examination staff of supervisory expectations and the appropriate utilization of guidance by March 30, 2008.

## MANAGEMENT RESPONSE TO RECOMMENDATIONS

This table presents the management response on the recommendations in our report and the status of the recommendations as of the date of report issuance.

<b>Rec. No.</b>	<b>Corrective Action: Taken or Planned</b>	<b>Expected Completion Date</b>	<b>Monetary Benefits</b>	<b>Resolved:<sup>a</sup> Yes or No</b>	<b>Open or Closed<sup>b</sup></b>
1 and 2	DSC will remind examination staff of supervisory expectations and the appropriate utilization of guidance.	March 30, 2008	\$0	Yes	Open

<sup>a</sup> Resolved – (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.

(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.

(3) Management agrees to the OIG monetary benefits, or a different amount, or no (\$0) amount. Monetary benefits are considered resolved as long as management provides an amount.

<sup>b</sup> Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.