Office of Inspector General

March 2007
Report No. 07-009

FDIC's Contract Planning and Management for Business Continuity

AUDIT REPORT

Office of Audits

OIG

Office of Audits

Report No. 07-009
March 2007

FDIC's Contract Planning and Management for Business Continuity

Results of Audit

The FDIC has planned to ensure contract services are provided in the event of an emergency and is continuing to improve contract management for business continuity. The FDIC has identified most essential contracts for business continuity purposes and modified many of those contracts to include emergency preparedness clauses. Also, the FDIC has a process to update its list of essential contracts in the BCP annually. The FDIC could further improve its contract planning and management for business continuity by:

- enhancing BCP procedures and the Business Impact Analysis questionnaire to require documentation of all essential contracts, including detailed information about each contract;
- requiring program offices to include emergency preparedness clauses in the Statement of Work for essential contracts and subcontracts to ensure that business continuity is considered in the procurement process; and
- amending acquisition policy and procedures and BCP policy to require that essential contractors (a) have emergency plans for providing services to the FDIC in the event of a disruption of normal operations and (b) participate in the FDIC's business continuity testing, training, and exercise activities.

Additional guidance in the FDIC's *Acquisition Policy Manual* and BCP policy and procedures would help to ensure that contractor activities are fully integrated into FDIC business continuity planning to enhance the FDIC's readiness to continue essential operations in emergency situations.

Recommendations and Management Response

We made three recommendations to strengthen the FDIC's contract planning and management for business continuity. DOA concurred with our recommendations and has completed corrective actions.

Background and Objective of the Audit

The Federal Emergency Management Agency issued Federal Preparedness Circular 65 (FPC 65), providing guidance for agencies to use in developing continuity of operations plans. The FDIC's Emergency Preparedness Program establishes the FDIC's business continuity policy and requires Business Continuity Plans (BCP) to be established in the FDIC's Washington Area Headquarters Offices and in each of the regional offices. The BCPs include procedures for relocating essential personnel; resuming and restoring FDIC critical business processes; and recovering and reconstituting supporting information technology systems. Identifying essential contracts and ensuring that contracts provide for services in the event of a BCP scenario are critical to FDIC operations.

The objective of this audit was to determine whether the FDIC has planned for essential contract services to be provided in the event of an emergency that requires implementation of the FDIC's BCP.

To view the full report, go to www.fdicig.gov/2007reports.asp

TABLE OF CONTENTS

ACRONYMS

APM	Acquisition Policy Manual
ASB	Acquisition Services Branch
BCP	Business Continuity Plan
BIA	Business Impact Analysis
COOP	Continuity of Operations Plan
DOA	Division of Administration
DIT	Division of Information Technology
EPP	Emergency Preparedness Program
ERP	Emergency Response Plan
FEMA	Federal Emergency Management Agency
FFIEC	Federal Financial Institutions Examination Council
FPC	Federal Preparedness Circular
GSA	General Services Administration
GPRA	Government Performance and Results Act
ISC	Infrastructure Services Contract
IT	Information Technology
ITAS	Information Technology Applications Systems
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SEPS	Security and Emergency Preparedness Section
SRA	SRA International, Inc.

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits
Office of Inspector General

DATE: March 30, 2007

MEMORANDUM TO: Arleas Upton Kea, Director
Division of Administration

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

SUBJECT: *FDIC's Contract Planning and Management for Business Continuity* (Report No. 07-009)

This report presents the results of our audit of the FDIC's Contract Planning and Management for Business Continuity. As of December 31, 2006, the FDIC had eight contracts valued at more than $800 million that were deemed essential to its critical business processes. The objective of this audit was to determine whether the FDIC has planned for essential contract services to be provided in the event of an emergency that requires the implementation of the *FDIC's Business Continuity Plan* (BCP).[1] Additional details on our objective, scope, and methodology are provided in Appendix I.

BACKGROUND

In June 2004, the Federal Emergency Management Agency (FEMA) revised Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations*,[2] to assist Federal Executive Branch departments, agencies and independent organizations in developing contingency plans and programs for the continuity of operations (COOP)[3] and to identify elements of a viable COOP capability.

Elements of a Viable COOP Capability

- ***Essential Functions***
- ***Plans and Procedures***
- ***Orders of Succession***
- ***Delegations of Authority***
- ***Alternate Facilities***
- ***Redundant Emergency Communications***
- ***Vital Records***
- ***Testing, Training, and Exercises***

Source: FPC 65.

FPC 65 states that COOP planning includes the activities of individual departments and agencies and their subcomponents to ensure that their essential functions are performed during any emergency or

[1] The FDIC's contract planning and management for business continuity was also addressed in a previous FDIC Office of Inspector General (OIG) report, *FDIC's Business Continuity Plan* (Report No. 04-029, dated August 9, 2004), which discusses the OIG's assessment of the FDIC's BCP against 14 key elements of business continuity planning.
[2] The FDIC has determined that FPC 65 contains guidance, not legally binding requirements, for the FDIC.
[3] The terms COOP and BCP are generally considered synonymous.

situation that may disrupt normal operations. FPC 65 further states that COOP planning (1) is part of the fundamental mission of federal agencies as responsible and reliable public institutions and (2) requires a comprehensive program to ensure the continuity of essential federal functions.

FDIC Emergency Preparedness

FDIC Circular 1500.5, *FDIC Emergency Preparedness Program*, dated January 30, 2007, serves as the official policy for FDIC Headquarters and regional offices in developing, implementing, and maintaining an FDIC Emergency Preparedness Program (EPP) to safeguard personnel and continue critical business processes during emergencies. The circular was updated during our audit, and the OIG provided comments during the revision process. FDIC Circular 1500.5 states that the EPP supports emergency preparedness planning guidance as outlined in FPC 65, as well as industry-recognized emergency preparedness best practices. Three components comprise the EPP: the Emergency Response Plan (ERP), a BCP, and any other plans necessary to prepare for an emergency. The ERP documents the procedures and structure for a coordinated response to an emergency and focuses on mitigating injuries and loss of life to FDIC personnel, contractors, and visitors at FDIC locations. The BCP documents the procedures for relocating essential personnel; resuming and restoring FDIC critical business processes; and recovering and reconstituting supporting information technology (IT) systems. The BCP is composed of individual division and office continuity plans, which identify critical business functions; how soon those functions must be operational in emergency situations; and the personnel, equipment, and systems resources needed to operate those functions during an emergency. The FDIC updates its BCP annually, as discussed below.

Business Impact Analysis

FPC 65 provides that planning requirements for a viable COOP capability must include the development, maintenance, and annual review of agency COOP capabilities using a multi-year strategy and program management plan. The FDIC addresses this requirement in the EPP by requiring an annual Business Impact Analysis (BIA). The BIA is a tool that enables full characterization of system requirements, processes, and interdependencies to determine contingency requirements and priorities. The BIA's purpose is to correlate specific system components with the critical services they provide, and based on that information, to characterize the consequences of a disruption to the system components.

Business Impact Analysis Objectives

- ***Identifying and prioritizing essential functions, business processes, and mission-critical applications***
- ***Defining the criticality criteria***
- ***Determining the disaster cost impact on business processes***
- ***Identifying critical application interdependencies***
- ***Defining recovery windows for critical applications***

Source: FDIC Circular 1500.5.

During the BIA, critical business function requirements and critical IT applications are reviewed, validated, added, or removed. The Division of Administration (DOA) is responsible for conducting an annual BIA with the FDIC's divisions and offices. The BIA serves as the basis for updating the corporate BCP and, as required, BCPs for the FDIC's divisions, offices, and regions.

Each year, the Directors of DOA and the Division of Information Technology (DIT) issue a BIA letter and BIA questionnaire to each FDIC division and office, informing them that BCPs will be updated based on completion of the annual BIA. The BIA letter notifies the divisions that DOA's Security and Emergency Preparedness Section (SEPS) and DIT security personnel will be meeting with them to obtain updated information on their critical business functions and resources requirements to accomplish these critical functions.

The BIA questionnaire obtains information on the: resources, assets, and applications that are critical to the divisions and offices and to the mission of the FDIC. During BIA meetings, SEPS and DIT personnel obtain additional detailed information on the functions the divisions and offices would require in an emergency, such as personnel, equipment, facilities, records, systems, interdependencies, and essential contracts and points of contact. The divisions and offices return the completed questionnaires to SEPS and DIT which, together with the results of the BIA meetings, are used in updating BCPs.

Business Continuity Planning

According to FDIC Circular 1500.5, the BCPs are the components of the EPP that document the procedures for relocating essential personnel, resuming and restoring FDIC critical business processes, and recovering and reconstituting supporting IT systems. The FDIC's division and office Directors, Regional Directors, and Managers are required to develop BCPs that can facilitate the resumption of critical business processes within 12 hours of plan activation and are capable of sustaining operations for up to 30 days. These BCPs are included in the corporate BCP. Each BCP must be reviewed by the Assistant Director, SEPS, for final approval by the FDIC Chairman or designee. The current corporate BCP was revised during 2006 and was issued on February 12, 2007.

Key Elements of the FDIC's Business Continuity Plan

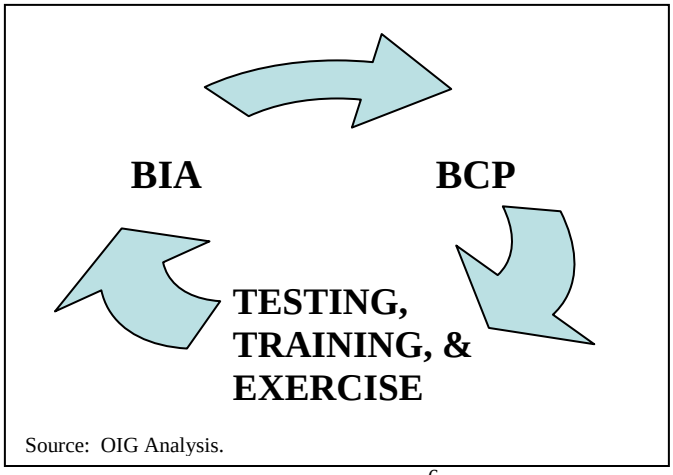
- ***Continuity Roles and Responsibilities***
- ***Orders of Succession***
- ***Plan Activation Criteria***
- ***Alert and Notification Procedures***
- ***Alternate Operating Facility Designation***
- ***Prioritized list of Essential Functions***
- ***Identification of Key Contractors***
- ***Interoperable Emergency Communications***
- ***Training and Exercise Events***

Source: FDIC Circular 1500.5.

The Headquarters BCP has identified a primary and secondary alternate facility for critical personnel if the FDIC Headquarters in Washington, D.C., is inaccessible or uninhabitable. Also, each regional office has a designated alternate worksite for relocating critical personnel if the vicinity surrounding a regional office becomes inaccessible or uninhabitable.

Identification of Essential Contracts. FDIC Circular 1500.5 states that BCPs should identify key contractors needed to operate during an emergency. Such contractors provide essential services in support of the FDIC's business processes. For example, the FDIC relies on contractors to support its designated alternate locations in the event of an emergency. The FDIC conducted a review of contracts during 2005 to identify those considered essential for business continuity. Specifically, contracts for IT support and maintenance, security services, call center

operations, fuel and facilities, shuttle services, cafeteria operations, and others were identified as essential. Once essential contracts had been identified, the FDIC's Legal Division worked with DOA's Acquisition Services Branch (ASB)[4] to draft emergency preparedness clauses to be added as modifications to the FDIC's essential contracts in accordance with the acquisition process outlined in the FDIC's *Acquisition Policy Manual* (APM),[5] which governs contracting activities. The list of essential contracts and emergency points of contact were then added to the FDIC's Headquarters BCP. The FDIC plans to use the annual BIA process to update the list of essential contracts used in BCPs. The Assistant Director, SEPS, stated that although SEPS is responsible for preparing the corporate BCP, the divisions are responsible for determining those contracts they consider essential and for ensuring that ASB adds contract clauses addressing business continuity to the essential contracts.



Source: OIG Analysis.

BCP Testing, Training, and Exercise

FPC 65 states that testing, training, and exercise are essential to demonstrating, assessing, and improving the ability of agencies to execute their COOP plans. FDIC Circular 1500.5 identifies the linkage of the processes for BIAs; BCPs; and testing, training, and exercise designed to maintain a viable emergency response capability. The BCPs at FDIC Headquarters and the regional offices are tested annually through table-top[6] and situation room[7] exercises to validate information in the BCP. Lessons learned from these exercises are then incorporated into the plans accordingly.

In addition, Headquarters and the regional office staff plan to participate in local exercises sponsored by various agencies, including the FEMA and the Federal Executive Councils located in major U.S. cities. SEPS advised us that it does not perform testing of essential contractor emergency response activities, and such testing is not currently required by the FDIC's Circular 1500.5. However, SEPS is responsible for the Security Guard contract, which supports all corporate components and has verified that the contractor has a plan that will provide guards in an emergency situation.

[4] ASB is responsible for fulfilling the FDIC's procurement responsibilities, including issuing policies and procedures governing contracts for goods and services.
[5] The APM establishes an updated set of policies and procedures for: (a) procuring goods and services on behalf of the Corporation in its corporate, receivership, and conservatorship capacities; and (b) identifying roles and responsibilities for all FDIC employees involved in the pre-solicitation, solicitation, proposal evaluation, award, and contract administration phases of the procurement process.
[6] Table-top exercises involve a test moderator setting forth a disaster scenario and the various recovery teams walking through their documented tasks in responding to the particular situation with an eye toward correcting any shortcomings in either the strategy or planned response.
[7] Situation room exercises include table-top exercises and engage some or all of the recovery strategy such as routing actual telecommunications traffic to the alternate facility.

RESULTS OF AUDIT

The FDIC has planned for essential contract services to be provided in the event of an emergency that requires implementation of the FDIC's corporate BCP. The FDIC established a process for performing BIAs; business continuity planning; and testing, training, and exercise activities that considers essential contract services. Also, the FDIC has identified most of its essential contracts for business continuity purposes and modified many of those contracts to include emergency preparedness clauses and plans to update FDIC essential contracts during the Corporation's 2007 BIA process. However, as summarized in the table below, the FDIC could further improve its contract planning and management for business continuity by including additional controls in the FDIC's EPP and APM related to essential contractors and subcontractors. These improvements will help to ensure that essential contractors are more fully integrated into the FDIC's business continuity activities to provide services in emergency situations.

Summary of Results of Audit

FDIC Process	FDIC Procedures for Essential Contractors	Improvement Needed
Business Impact Analysis	Essential functions are reviewed and updated during the annual BIA process.	The BIA questionnaire does not solicit key information on essential contractors and subcontractors.
Business Continuity Planning	Emergency preparedness clauses are included in essential contracts.	The APM does not include a requirement for contracts to be evaluated to determine whether emergency preparedness clauses should be included for prime contractors and subcontractors during preparation of the contract Statements of Work.
Testing, Training, and Exercise	The EPP requires regularly-scheduled training and exercise events such as table-top and functional exercises and personnel recall roster tests.*	Essential contractors are not required to submit their emergency plans for FDIC functions for review and incorporation, as appropriate, into the FDIC's BCPs. Essential contractors do not participate in FDIC BCP testing, training, and exercises.

* Recall rosters list essential FDIC senior management and personnel who are notified by electronic means to report to a designated location in the event of an emergency or implementation of the FDIC's BCP.

BUSINESS IMPACT ANALYSIS

Although SEPS and DIT have identified most of the FDIC's essential contracts, the current BIA questionnaire does not solicit key information on these contracts. The FDIC's EPP was revised in January 2007 to include procedures for identifying essential contractors. However, the procedures for conducting the BIA, dated November 19, 2003, do not contain provisions dealing with essential contractors' support such as contractor emergency plans; essential subcontracts; and testing, training, and exercise requirements. As a result, the FDIC's BIA process may not fully document or consider information that can be useful in planning for essential contract services in an emergency.

Use of Emergency Preparedness Clauses

FDIC Circular 1500.5 focuses attention on business continuity planning as the means for resuming and restoring critical business processes during an emergency. The FDIC uses the BIA to make annual updates to the BCPs. The FDIC relies extensively on contractors; therefore, contractor support is a key component of the BIA and business continuity planning.

We also reviewed the best practices for financial institutions as described in the Federal Financial Institutions Examination Council (FFIEC) *Business Continuity Planning IT Examination Handbook*, issued in March 2003. The FFIEC provides guidance to financial institutions and examiners on evaluating financial institution and service provider risk management processes, including guidance on conducting the BIA. The focus is on business continuity planning, whereby financial institutions ensure the maintenance or recovery of operations when confronted with adverse events, such as natural disasters, technological failures, human error, or terrorism.

The FFIEC recommends that financial institutions ensure that key contractors/service providers are identified and backup arrangements are stipulated in contracts for services. The FFIEC also recommends that the BIA should solicit the critical outsourced relationships and dependencies and that each department should document the mission-critical functions performed by these outsourced relationships. Further, the FFIEC recommends that personnel responsible for the BIA consider developing uniform interview and inventory questions that can be used on an enterprise-wide basis. Uniformity can improve the consistency of responses and help personnel involved in the BIA phase to compare and evaluate business process requirements. The FFIEC handbook indicates that the BIA should solicit the critical outsourced relationships and dependencies.

The SEPS and DIT personnel who conducted the BIA provided us with a detailed description of the process and told us that although the BIA procedures and questionnaire do not include questions on essential contracts, SEPS and DIT plan to discuss essential contracts during their BIA meetings with the divisions and offices. SEPS stated that the name of the contract and the contractor key points of contact are included in the BCP.

To help ensure that critical information on essential contractors is obtained during the BIA and a standard procedure is used for updating essential contractor information in the BCP, the FDIC's

policy and procedures for conducting the BIA and the BIA questionnaire could be amended to solicit additional information about essential contracts such as:

- the purpose of the contract;
- how the contractor may need to alter operations for the FDIC in an emergency;
- the critical services required from contractor personnel and potential disaster cost impact;
- the timeframes during which the services would be required and system recovery windows;
- whether the contractor is required to have an emergency plan that addresses FDIC activities and to submit the plan to the FDIC for review;
- whether the contract includes an emergency preparedness clause;
- essential subcontracts; and
- testing, training, and exercise requirements for the contractors' support provided to the FDIC.

Obtaining responses to these questions and others determined to be important in the BIA questionnaire would result in more complete information for the FDIC's business planning activities, consistency and uniformity in information obtained, and assistance to program managers in identifying essential contracts and subcontracts. This information would also facilitate the consideration of contractor support in testing, training, and exercise activities.

Recommendation

(1) We recommend that the Director, DOA, amend, as appropriate, the BIA procedures and questionnaire for obtaining additional information on essential contracts and for using the contractor-related responses in the BCP.

BUSINESS CONTINUITY PLANNING

The FDIC could improve its contract planning for business continuity to ensure all essential contractors and subcontractors are required to provide services for the FDIC in an emergency. The EPP includes requirements for the identification of essential contractors needed to operate during an emergency. However, APM contracting procedures do not require that program officials determine whether a contract is essential for business continuity when preparing a Statement of Work for the contract. In 2005, DOA completed a review of essential contracts and modified them to include an emergency preparedness clause. However, contracts awarded since the DOA contract review that may be essential to the FDIC's mission had been awarded without an emergency preparedness clause. Also, the FDIC has not established procedures to ensure that key subcontractors on the FDIC's essential contracts are prepared to provide essential services in an emergency. As a result, essential contractors and subcontractors may not be routinely identified as part of the procurement process for purposes of business continuity planning activities, and the scope of their emergency responsibilities may not be well defined.

Contracting Procedures for Essential Services

During 2005, SEPS and DIT determined that eight contracts were essential for business continuity. Because DOA had not established a procedure for evaluating whether contracts were essential for business continuity when originally awarded, these contracts did not include an

emergency preparedness clause. Instead, partly in response to an FDIC OIG report, *FDIC's Business Continuity Plan* (Report No. 04-029, dated August 9, 2004), SEPS and DIT determined which contracts were essential and then modified those contracts to include an emergency preparedness clause as follows.

> If, at any time during the performance of this contract, the FDIC requires services essential or critical to its mission due to an actual or threatened emergency situation as declared by the federal, state, or local authority, the contractor shall provide all resources necessary to support these services. If an actual or threatened emergency exists, the contractor shall take immediate and effective measures to ensure the availability or use of back-up or redundant services to support the emergency situation without any disruption. Any needed back-up or redundant services shall be provided for as long as the actual or threatened emergency situation exists.
>
> Any costs associated with providing back-up or redundant services shall be reimbursed at the previously negotiated labor rates. After receipt of the FDIC's notification requiring services essential or critical to its mission, the contractor shall submit an equitable adjustment proposal for the back-up or redundant services. The equitable adjustment proposal shall include, as a minimum, a breakdown of the labor categories involved, the total estimated hours for each labor category, the negotiated labor rate, and the total cost/price.

The APM does not require the routine identification of essential contracts. Therefore, new contracts may not include emergency preparedness requirements. For example, DIT's Information Technology Applications Systems (ITAS) contract, which totals $554.8 million for IT systems development and maintenance, was not awarded until after the 2005 identification process had been completed and was not modified to include the emergency preparedness clause.

While SEPS and DIT personnel plan to include questions about essential contracts in their future BIA interviews, the BIA was not conducted during 2006 because of the FDIC's move to Virginia Square. As of February 1, 2007, the ITAS contract had been in effect for 19 months without an emergency preparedness clause.

The ITAS contract is a multi-vendor contract with 4 contractors and 18 current task orders. According to DIT, some of the task orders provide essential support to DIT and should include the emergency preparedness clauses. If FDIC contracting procedures had required that program officials include emergency preparedness clauses in contracts and task orders that provide essential support, program officials would be on notice of such a requirement and could have taken the steps necessary to ensure that the contractors were prepared to provide such critical services for FDIC's IT systems. The FDIC's ability to maintain critical operations during an emergency could be improved by ensuring that all essential contracts include the appropriate emergency preparedness/business continuity clauses. This can be accomplished by including emergency preparedness provisions in the Statement of Work for essential contracts as part of the solicitation process for contractor proposals.

Contracting Procedures for Subcontractors

The FDIC has not established procedures or taken action to ensure that key subcontracts for the FDIC's essential contracts include emergency preparedness clauses. As discussed earlier, the FDIC has identified eight contracts that are considered essential to maintain the FDIC's critical functions in the event of an emergency or business continuity scenario. Two of these eight contracts are critical to the FDIC's IT systems and have multiple subcontractors. The FDIC has not required the prime contractors to ensure that subcontracts for work on essential FDIC contracts have emergency preparedness requirements. Therefore, the FDIC does not have full assurance that the prime contractor will be able to perform in cases where subcontractors provide critical support to essential prime contractors.

The following examples illustrate the need for consideration of subcontractor emergency preparedness requirements. DIT has an Interagency Agreement with the General Services Administration (GSA), through which a task order, the *Infrastructure Services Contract* (ISC) was awarded to SRA International, Inc. (SRA). This contract was awarded in September 2004 and was modified in May 2006 to include the emergency preparedness clause that had been added to the FDIC contracts that had previously been identified as being essential for business continuity. The SRA contract has an expenditure ceiling totaling $341 million and includes services provided by three SRA subcontractors. Subcontracted services included work for helpdesk and client support, mainframe operations, and telecommunications support services that may be essential for business continuity. In addition, SRA used some short-term labor contracts related to IT security and mainframe support. However, according to the DIT's Oversight Manager for the contract, none of the SRA's subcontracts had been amended to include the emergency preparedness clause when the overall contract was modified in 2006.

Also, as previously discussed, DIT's ITAS contract does not contain the emergency preparedness clause, and it is a multi-vendor contract with 4 contractors and 18 current task orders. As a result of our audit work, the DIT Oversight Manager advised us that he was going to request that ASB modify the ITAS contract to include the emergency preparedness clause. However, the FDIC does not have a policy or procedures for ensuring that the prime contractors include the clause in their subcontracts or to provide for other arrangements to ensure that subcontractors fulfill their responsibilities in providing services. Because the SRA and the ITAS contractors have not included the emergency preparedness clause in their essential subcontracts, the FDIC's ability to fully provide services in an emergency may be compromised.

Recommendation

(2) We recommend that the Director, DOA, amend the procedures in the *Acquisition Policy Manual*, or other procedures as appropriate, to require that Statements of Work for contracts and task orders under contracts contain:

- business continuity requirements if contracted services are deemed essential in the event of an emergency or business continuity event,

- requirements that essential contractors include emergency preparedness and business continuity provisions in essential subcontracts.

BCP PROCEDURES FOR CONTRACTOR TESTING, TRAINING, AND EXERCISES

The FDIC has not established procedures requiring essential contractors to provide the FDIC with evidence of their emergency plans for FDIC critical business functions or for participation in the FDIC's BCP testing, training, and exercises. According to SEPS, ASB, and Legal Division personnel, the FDIC's practices for ensuring that essential contractors provide services in an emergency are limited to the inclusion of an emergency preparedness clause in the contract. This clause is intended to put contractors on notice that the services they provide are critical to the FDIC's mission and that the FDIC would require the continuation or expansion of these services in an emergency. However, without verifying contractors' emergency plans for FDIC critical functions and including contractors in FDIC BCP testing, training and exercises, the FDIC does not have adequate assurance that essential contractors will be able to provide the FDIC the service coverage that may be required during a business continuity scenario.

Testing, Training, and Exercises

FDIC Circular 1500.5 requires that the Assistant Director, SEPS, coordinate and facilitate emergency preparedness training and exercise events. Specifically, the circular requires that the Assistant Director develop strategies for maintaining a viable emergency response capability that includes training and exercise activities and milestones, coordinating with senior FDIC management on these activities, and identifying and resolving resulting issues and concerns. The circular also refers to testing with respect to the use of recall rosters. Since the FDIC relies extensively on essential contractors, contractor support is a key component of the FDIC's emergency response capability.

In addition to reviewing the requirements of FDIC Circular 1500.5, we reviewed the best practices for financial institutions described in the FFIEC *Business Continuity Planning, IT Handbook*. The FFIEC recommends that financial institutions obtain a copy of vendors' BCPs and incorporate them into their business continuity plans. The FFIEC also recommends that contracts address the service providers' responsibilities for maintenance and testing of disaster recovery and contingency plans and that, if possible, respective institutions should consider participating in their service providers' testing process. While the FDIC is not required to follow the FFIEC guidance, industry best practices recommend that essential contracts be identified and their business continuity plans be tested to ensure the continuity of operations.

Although the FDIC has conducted business continuity exercises to test the FDIC's BCPs, the FDIC has not included contractors' business continuity activities in any of these events. Further, the FDIC does not have policies and procedures in its APM to address contractors' emergency planning and the verification of the contractors' operational capacities through testing, training, and exercises to determine whether the contractors have the ability to provide services expected by the FDIC in the event of an emergency.

For most of the contracts identified as essential, DOA has submitted an emergency preparedness clause to the contractor for concurrence and inclusion in a contract modification. Nevertheless, with the exception of one essential contract related to the FDIC's Call Center,[8] the FDIC has not requested that the other essential contractors provide their emergency plans for FDIC review or required that essential contractors affirm that their organization has a business continuity or emergency preparedness plan. The one contract that does require the contractor to provide its emergency plan resulted from the initiative of the individual contract manager and not in response to FDIC's policies or procedures.

According to SEPS and Legal Division personnel, including contractors in emergency preparedness testing, training, and exercises has not been discussed or recommended to FDIC senior management. Also, Circular 1500.5 does not specifically refer to including contractors in these activities. However, as part of fulfilling its overall responsibilities for testing, training, and exercises of business continuity planning, the FDIC could more fully consider its reliance on essential contractors and the need to assess their capabilities, including those of their essential subcontractors, to respond in the event of an emergency. Doing so will help ensure available emergency response capability.

Recommendation

(3) We recommend that the Director, DOA, amend:

- procedures in the *Acquisition Policy Manual*, or other procedures as appropriate, to provide that Statements of Work for essential contracts and task orders ensure that contractors have emergency plans for providing services to the FDIC in the event of a disruption of normal operations and participate in the FDIC's business continuity testing, training, and exercises.

- Circular 1500.5, *FDIC's Emergency Preparedness Program*, to include essential contractors in FDIC's BCP planning and testing, training, and exercises.

CORPORATION COMMENTS AND OIG EVALUATION

The Director, DOA, provided a written response, dated March 30, 2007, to a draft of this report. DOA's response is presented in its entirety in Appendix II. DOA concurred with each of the three recommendations and has taken the following corrective actions:

- revised the BIA questionnaire for immediate use. The questionnaire includes the identification of critical contractor/subcontractor staff and whether they have an Emergency Plan which can be incorporated into the FDIC Business Continuity Plan.

- updated the Requirements Package Checklist in the APM to include the requirement that any Statement of Work for essential services contain business continuity requirements as well as emergency preparedness and business continuity provisions in essential

[8] The FDIC Call Center is the primary telephone point of contact for the banking industry and the general public. It is critical to the FDIC's mission because it assists in maintaining public confidence in the nation's financial system.

subcontracts. Additionally, the checklist was updated to require that essential contractors participate in the FDIC's business continuity planning, testing, training, and exercises.

- revised Circular 1500.5, entitled *FDIC's Emergency Preparedness Program* to include essential contractors in FDIC's BCP planning, testing, training, and exercises.

DOA's actions effectively address the recommendations, and we consider all the recommendations closed. Appendix III presents a summary of DOA's responses to our recommendations and the corrective actions taken.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether the FDIC has planned for essential contract services to be provided in the event of an emergency that requires the implementation of the BCP. Our scope was limited to the contracts identified by SEPS and the DIT Security Section as essential for business continuity and that are included in the FDIC's Headquarters BCP as of December 1, 2006. We conducted the audit from November 2006 through January 2007 in accordance with generally accepted government auditing standards.

To accomplish our objective, our methodology included reviewing the following documents:

- FDIC Circular 1500.5, *FDIC Emergency Preparedness Program*, dated December 28, 2004, and the revised Circular 1500.5, dated January 30, 2007. (The provisions outlined in this circular serve as the official policy for FDIC Headquarters and regional offices in developing, implementing, and maintaining a BCP.)
- FEMA FPC 65 *Federal Executive Branch Continuity of Operations*.
- GSA's *Occupant Emergency Program Guide*.
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, *Contingency Planning Guide for Information Technology Systems*.
- FFIEC's *Business Continuity Planning IT Examination Handbook*, issued March 2003.
- Certified Information Systems Auditor Review Manual 2006, *Business Continuity and Disaster Recovery*.
- Appendix III to the U.S. Office of Management and Budget Circular No. A-130, *Security of Federal Automated Information Resources.*
- FDIC's *Procedure for Conducting a Business Impact Analysis*, dated November 19, 2003.
- FDIC OIG's Evaluation Report, Number 04-029 entitled, *FDIC's Business Continuity Plan*, dated August 9, 2004; and FDIC OIG's Evaluation Report, Number 03-042 entitled, *Business Continuity Planning at FDIC-Supervised Institutions*, dated September 25, 2003.

To identify FDIC procedures and practices for contract planning and management for business continuity, we obtained information from the following FDIC officials:

- Assistant Director, Security and Emergency Preparedness Section, DOA
- Chief, Transportation and Emergency Response Unit, DOA
- Assistant Director, IT Contracting Section, DOA
- Assistant Director, ASB, DOA
- Procurement Analyst, ASB, DOA
- Contract Oversight Manager, DIT
- Chief Oversight Support Section, DIT
- Supervisory IT Specialist, Security Section, DIT
- Senior IT Specialist, Security Section, DIT
- Senior Counsel, Legal Division

Our methodology did not include a review of the FDIC's BCP, which was being revised during our audit.

Internal Management Controls

We evaluated the effectiveness of controls in place for identifying essential contracts for business continuity and ensuring emergency preparedness clauses had been included in contracts deemed essential for business continuity. These controls included the policies and procedures for conducting a BIA and BCP. In the absence of written policies, we relied on interviews and information obtained from the Assistant Director, SEPS, who is responsible for the FDIC's BCP, and other DOA and DIT officials.

Compliance With Laws and Regulations

We coordinated reviews of laws, directives, and plans with the OIG's Office of Counsel to determine applicability to the FDIC and to gain an understanding of applicable laws and regulations. We found no instances where the FDIC was not in compliance with applicable laws and regulations.

Government Performance and Results Act, Computer-Processed Data, and Fraud or Illegal Acts

We reviewed DOA's performance measures under the Government Performance and Results Act, Public Law 103-62 (GPRA). We reviewed the FDIC's 2006 Annual Performance Plan and the FDIC's Strategic Plan for 2005-2010 to determine whether the FDIC has established goals related to contract planning and management for business continuity. Neither plan includes goals, objectives, or indicators specifically related to the subject of our audit.

We did not rely on computer-processed data to support our significant conclusions, findings, and recommendations, and, as a result, did not perform work to determine the reliability of such data.

Our audit program included steps for providing reasonable assurance of detecting fraud or illegal acts, and none came to our attention.

CORPORATION COMMENTS

FDIC
Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Division of Administration

March 30, 2007

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

FROM: Arleas Upton Kea
Director, Division of Administration

SUBJECT: Management Response to the Draft OIG Audit Report Entitled, *FDIC's Contract Planning and Management for Business Continuity* (Assignment No. 2007-003)

This is in response to the subject Draft Office of Inspector General (OIG) Report issued February 26, 2007. In its report, the OIG identified three recommendations.

We appreciate that the OIG noted that the FDIC has planned for essential contract services to be provided in the event of an emergency but recognize that some improvements can be made in contract planning and management for business continuity. This response outlines our planned corrective actions for each of the recommendations cited in the OIG's Report.

MANAGEMENT DECISION

Finding: Business Impact Analysis

Condition: By not soliciting key information on FDIC essential contracts on the BIA questionnaire, the BIA process may not fully document or consider information that can be useful in planning for essential contract services in an emergency.

Recommendation 1: That the Director, Division of Administration (DOA), amend, as appropriate, the BIA procedures and questionnaire for obtaining additional information on essential contracts and for using the contractor-related responses in the BCP.

Management Response 1: DOA concurs with this recommendation. The DOA, Security and Emergency Preparedness Section revised the BIA questionnaire. The questionnaire includes the identification of critical contractor/subcontractor staff and whether they have an Emergency Plan which can be incorporated into the FDIC Business Continuity Plan. This questionnaire was revised March 13, 2007, for immediate use.

Finding: Contracting Procedures for Essential Services

Condition: Essential contractors and subcontractors may not be routinely identified as part of the procurement process for purposes of business continuity planning activities.

Recommendation 2: That the Director, DOA, amend the procedures in the Acquisition Policy Manual (APM), or other procedures as appropriate, to require that Statements of Work for contracts and task orders under contracts contain:

- A) Business continuity requirements if contractor services are deemed essential in the event of an emergency or business continuity event,

- B) Requirements that essential contractors include emergency preparedness and business continuity provisions in essential subcontracts.

Management Response 2: DOA concurs with this recommendation. DOA's Acquisition Services Branch updated the Requirements Package Checklist in the APM to include the requirement that any statement of work for essential services contain business continuity requirements as well as emergency preparedness and business continuity provisions in essential subcontracts. The updated checklist was issued through Interim Acquisition Policy Memo #2007-1 on March 21, 2007.

Finding: Testing, Training, and Exercises

Condition: Without verifying contractors' emergency plans for FDIC critical functions and including contractors in FDIC BCP testing, training and exercises, the FDIC does not have adequate assurance that essential contractors will be able to provide the FDIC the service coverage required during a business continuity scenario.

Recommendation 3: That the Director, DOA, amend:

- A) Procedures in the *Acquisition Policy Manual*, or other procedures as appropriate, to provide that Statements of Work for essential contracts and task orders ensure that contractors have emergency plans for providing services to the FDIC in the event of a disruption of normal operations and participate in the FDIC's business continuity testing, training, and exercises.

- B) Circular 1500.5, *FDIC's Emergency Preparedness Program*, to include essential contractors in FDIC's BCP planning and testing, training, and exercises.

Management Response 3A: DOA concurs with this recommendation. DOA's Acquisition Services Branch updated the Requirements Package Checklist in the APM to include the requirement that any statement of work for essential services contain requirements for the contractor to have emergency plans for providing services to the FDIC in the event of a disruption of normal operations and participate in the FDIC's business continuity planning, testing, training, and exercises. The updated checklist was issued through Interim Acquisition Policy Memo #2007-1 on March 21, 2007.

Management Response 3B: DOA concurs with this recommendation. DOA's Security and Emergency Preparedness Section revised Circular 1500.5, entitled *FDIC's Emergency Preparedness Program* on March 13, 2007; to include essential contractors in FDIC's BCP planning, testing, training, and exercises.

If you have any questions regarding this response, FDIC's point of contact for this matter is William Gately. Mr. Gately can be reached at (703) 562-2118.

cc: Michael J. Rubino
Trisha M. Bursey
William A. Kmetz
James H. Angel, Jr.

3

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.

Rec. No.	Corrective Action Taken	Completion Date	Monetary Benefits	Resolved: [a] Yes or No	Open or Closed
1	Revised the BIA questionnaire to include identification of critical contractor/subcontractor staff and whether they have an Emergency Plan which can be incorporated into the FDIC BCP.	March 13, 2007	N/A	Yes	Closed
2	Updated the Requirements Package Checklist in the APM to require that any Statement of Work for essential services contain business continuity provisions as well as emergency and business continuity provisions in essential subcontracts.	March 21, 2007	N/A	Yes	Closed
3	Updated the Requirements Package Checklist in the APM to require that any Statement of Work for essential services contain requirements for the contractor to have emergency plans for providing services to the FDIC in the event of a disruption of normal operations and to participate in the FDIC's business continuity planning, testing, training, and exercises.	March 21, 2007	N/A	Yes	Closed
	Revised Circular 1500.5 to include essential contractors in FDIC's BCP planning, testing, training, and exercises.	March 13, 2007	N/A	Yes	Closed

[a] 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.

[b] Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.