Office of Inspector General

September 2007
Report No. AUD-07-014

Independent Evaluation of the FDIC's Information Security Program-2007

AUDIT REPORT

Office of Audits

OIG

Office of Audits

OIG

Background and Purpose of Evaluation

The FDIC Office of Inspector General (OIG) contracted with KPMG, LLP (KPMG) to conduct an independent evaluation of the FDIC's information security program and practices pursuant to the Federal Information Security Management Act of 2002 (FISMA). FISMA requires federal agencies, including the FDIC, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluation to the Office of Management and Budget.

Key to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding the sensitive information it collects and manages in its role as federal deposit insurer of banks and savings associations. Ensuring the integrity, availability, and confidentiality of this information in an environment of increasingly sophisticated security threats requires a strong, enterprise-wide information security program.

The objective of the evaluation was to determine the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with the FISMA and related information security policies, procedures, standards, and guidelines.

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

Report No. AUD-07-014
September 2007

Independent Evaluation of the FDIC's Information Security Program-2007

Results of Evaluation

The FDIC has made significant progress in recent years in addressing the information security provisions of FISMA and the National Institute of Standards and Technology. This progress is noteworthy given the considerable increase in information-security-related requirements levied on federal agencies. KPMG found that the FDIC established policies and procedures in substantially all of the security control areas evaluated. In addition, KPMG noted particular strength in the areas of *Information Security Governance*, *Incident Response*, and *Awareness and Training* and that additional improvements were underway at the close of the evaluation.

These accomplishments are notable. However, as reflected in the table below, KPMG identified a number of information security control deficiencies warranting management attention. Addressing these security control deficiencies will contribute to the FDIC's ongoing efforts to achieve reasonable assurance of adequate security over corporate information resources. KPMG's report identifies steps that the Corporation can take to strengthen security controls in the priority areas of *Access Control*; *Identification and Authentication*; *Certification, Accreditation, and Security Assessments*; *Risk Assessment; Personnel Security;* and *Audit and Accountability*. In many cases, the FDIC was already working to improve security controls in these areas during KPMG's evaluation. The FDIC OIG will follow up on the security control deficiencies identified in this report as part of future FISMA evaluations.

KPMG's Assessment of the FDIC's Security Program Controls

Control Class	Control Families Tested That Demonstrated Effectiveness	Control Families Tested That Warrant Management Attention
Program	• Information Security Governance	• Enterprise Architecture
Management	• Planning	• Risk Assessment • Certification, Accreditation, and Security Assessments
Operational	• Contingency Planning • Configuration Management • Maintenance • Incident Response • Awareness and Training	• Physical and Environmental Protection • Personnel Security • System and Information Integrity • Media Protection
Technical		• Identification and Authentication • Access Control • Audit and Accountability

Source: KPMG's 2007 Evaluation of the FDIC's Information Security Program.

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226 Office of Inspector General

DATE: September 27, 2007

MEMORANDUM TO: Sheila C. Bair, Chairman
Federal Deposit Insurance Corporation

/Signed/
FROM: Jon T. Rymer
Inspector General

SUBJECT: *Independent Evaluation of the FDIC's Information Security Program—2007*
(Report No. AUD-07-014)

Attached is a copy of the subject report prepared by KPMG, LLP (KPMG) under contract with the Office of Inspector General (OIG). Please refer to the Executive Summary for the overall results.

The OIG provided you, the Chief Operating Officer, and Chief Financial Officer with a draft copy of this report on September 14, 2007. Because the report contains no recommendations, no written response was required from the Corporation. However, KPMG did consider and address, as appropriate, informal comments provided by FDIC officials. In response to a request from the Office of Management and Budget (OMB), the OIG reported separately on the status of the FDIC's privacy program in its report entitled, *Response to Privacy Program Information Request in OMB's Fiscal Year 2007 Reporting Instructions for FISMA and Agency Privacy Management* (Report No. AUD-07-013, dated September 26, 2007).

The OIG's independent security evaluation and privacy program reports, together with the FDIC Chief Information Officer's report required by the Federal Information Security Management Act of 2002, are due to the OMB by October 1, 2007.

The 2007 FISMA report will be made publicly available. If you have any questions concerning this report, please contact me at (703) 562-2166 or Russell A. Rau, Assistant Inspector General for Audits, at (703) 562-6350. We appreciate the courtesies extended to the audit staff and KPMG during this assignment.

Attachment

Independent Evaluation of the FDIC's Information Security Program-2007

Prepared for the Federal Deposit Insurance Corporation Office of Inspector General

September 26, 2007

KPMG LLP
2001 M Street, NW
Washington, DC 20036

Table of Contents

Table of Contents

FIGURES

KPMG LLP
2001 M Street, NW
Washington, DC 20036

EXECUTIVE SUMMARY

September 26, 2007

Honorable Jon T. Rymer
Inspector General
Federal Deposit Insurance Corporation
3501 Fairfax Drive
Arlington, VA 22226-3500

Dear Mr. Rymer:

This report presents the results of our independent evaluation of the FDIC's information security program and practices. The FDIC Office of Inspector General (OIG) contracted with KPMG to conduct a performance audit of the FDIC's information security program and practices pursuant to the Federal Information Security Management Act of 2002 (FISMA). We conducted our performance audit in accordance with *Generally Accepted Government Auditing Standards* issued by the Comptroller General of the United States. FISMA requires federal agencies, including the FDIC, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluation to the Office of Management and Budget (OMB). FISMA requires that the independent evaluation be performed by the agency Inspector General (IG) or an independent external auditor as determined by the IG.

The objective of KPMG's evaluation was to determine the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards, and guidelines. As part of its work, KPMG prepared responses to a series of security-related questions directed to agency IGs in OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The responses to OMB's questions are included in Appendix IV of this report. In addition, KPMG briefed the FDIC's Chief Information Officer and Director, Division of Administration, on the preliminary results of the evaluation on September 6, 2007. The purpose of the briefing was to provide these management officials with detailed information to facilitate the FDIC's ongoing efforts to strengthen its information security program controls. We consider the information provided during the briefing to be sensitive. Accordingly, that information is not included in this publicly available report.

As our report details, the FDIC continues to make significant progress in improving its information security program and practices and in addressing current and emerging information security standards and guidelines developed by the National Institute of Standards and Technology (NIST). However, KPMG identified a number of information security control deficiencies warranting management attention. Addressing these security control deficiencies will contribute to the FDIC's ongoing efforts to achieve reasonable assurance of adequate security over Corporate information resources. Listed on page 2, in priority order, are six steps that the Corporation can take to improve the effectiveness of its information security program controls. In many cases, the FDIC was already working to address these steps during KPMG's evaluation.

(1) Strengthen *Access Control* by (a) continuing to place priority attention on ongoing efforts to restrict user access to sensitive information stored on the Corporation's network shared drives, (b) disabling or deleting separated employees' user account access to applications in a timely manner, and (c) improving the separation of duties among the Windows network administrators.

(2) Strengthen *Identification and Authentication* controls by ensuring that passwords used to control access to critical information security resources, such as network servers, databases, and applications comply with FDIC policy.

(3) Enhance the effectiveness of the FDIC's information security vulnerability scanning processes by ensuring that all information technology (IT) equipment connected to the FDIC's network are routinely scanned with the appropriate user identification (ID) and password to identify missing security patches and security configuration errors.

(4) Strengthen *Personnel Security* controls by (a) assigning a high or moderate risk level designation to contractor employees with broad physical access permissions to FDIC headquarters facilities and confirming that the U.S. Office of Personnel Management (OPM) has sufficient contractor employee information to start the appropriate background investigation process before granting broad physical access, and (b) developing a process to assist in identifying employees and contractors with background investigations that are not commensurate with individual risk level designations.

(5) Strengthen *Audit and Accountability* controls by continuing to place priority attention on developing a risk-based enterprise-wide approach for (a) monitoring user access privileges in information systems and (b) generating and reviewing audit logs for the FDIC's inventory of information systems.

(6) Enhance the FDIC's ongoing security control assessments in each of the five areas listed above to provide greater assurance that such controls are operating effectively.

This performance audit did not constitute an audit of financial statements in accordance with *Generally Accepted Government Auditing Standards.* KPMG was not engaged to, and did not, render an opinion on the FDIC's internal controls over financial reporting or over financial management systems. KPMG cautions that projecting our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate. Appendix I of this report provides detailed information regarding the evaluation's objective, scope, and methodology, as well as additional information about information-security-related laws, regulations, and other guidance. Appendix II provides a status of prior year FISMA key steps to improve information security, and Appendix III includes a summary of the controls tested as part of the 2007 FISMA evaluation. Appendix IV is the response to OMB Security Questions, and Appendix V provides a glossary of terms.

Sincerely,

KPMG LLP

List of Acronyms

Acronym	Definition
ASA	Application Security Assessment
BCP	Business Continuity Plan
BIA	Business Impact Analysis
C&A	Certification and Accreditation
CD/DVD	Compact Disc/Digital Video Disc
CFO	Chief Financial Officer
CHRIS	Corporate Human Resources Information System
CIO	Chief Information Officer
CMMI	Capability Maturity Model Integration
COBIT®	Control Objectives for Information and related Technology
COO	Chief Operating Officer
CSIRT	Computer Security Incident Response Team
DIT	Division of Information Technology
DOA	Division of Administration
EA	Enterprise Architecture
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers' Financial Integrity Act
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
HSPD	Homeland Security Presidential Directive
ID	Identification

Acronym	Definition
IDS	Intrusion Detection System
IG	Inspector General
IRIS	Internal Risks Information System
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
IT	Information Technology
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action & Milestones
PUB	Publication
RCN	Remote Client Network
RUP®	Rational Unified Process
SDLC	System Development Life Cycle
SP	Special Publication
SQL	Structured Query Language
SSPs	System Security Plans
ST&E	Security Test & Evaluation
USB	Universal Serial Bus
U.S.C.	United States Code

BACKGROUND

Key to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding the sensitive information (including personally identifiable information (PII)) that the FDIC collects and manages in its role as federal deposit insurer of banks and savings associations. In addition, as an employer and acquirer of services, the FDIC obtains sensitive information from its employees and contractors. Implementing proper controls over this information is critical to mitigating the risk of an unauthorized disclosure that could lead to identity theft, consumer fraud, and potential legal liability or public embarrassment for the Corporation. Widely publicized reports of network compromises and data security breaches at federal agencies have raised concern among federal agencies, the public, and the Congress and underscore the importance of implementing strong, enterprise-wide information security controls. In addition, the U.S. Government Accountability Office (GAO) has designated information security as a government-wide, high-risk issue in its reports to the Congress since 1997.

In response to concerns about the security of federal information systems, the Congress enacted Title III of the E-Government Act of 2002, commonly referred to as FISMA. FISMA focuses on improving the oversight of federal information security programs and facilitating progress in correcting agency information security deficiencies. FISMA requires federal agencies, including the FDIC, to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[1] Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related policies, procedures, standards, and guidelines. FISMA directs agency heads to report annually to the OMB Director, Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

OMB is responsible for annually reporting to the Congress on agency compliance with FISMA's requirements. OMB relies on the annual agency FISMA reports to evaluate agency-specific and government-wide security performance. OMB provided federal agencies with instructions for satisfying their reporting requirements under FISMA in a July 25, 2007 memorandum, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. OMB's primary agency security policy is OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (OMB A-130, Appendix III), dated November 28, 2000.[2]

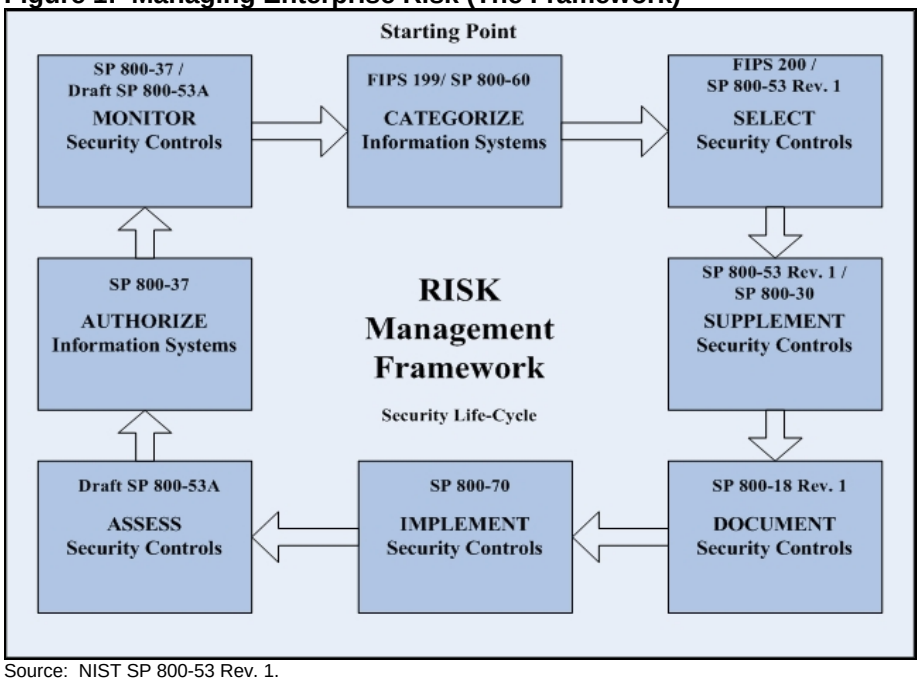
[1] The FDIC has determined that aspects of FISMA are legally binding on the Corporation.
[2] Various provisions of OMB A-130, Appendix III are legally binding on the FDIC.

NIST Security Standards and Guidelines

FISMA directs NIST to develop risk-based standards and guidelines to assist agencies in defining minimum security requirements for the non-national security systems used by agencies.[3] NIST has developed such standards and guidelines as part of its FISMA Implementation Project and is developing additional standards and guidelines. KPMG based its security evaluation primarily on the security controls defined in NIST Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and Special Publication (SP) 800-53 Revision (Rev.) 1, *Recommended Security Controls for Federal Information Systems*.[4] These NIST publications define a framework for protecting the confidentiality, integrity, and availability of federal information and information systems consisting of three general classes of security controls, namely, management, operational, and technical. Collectively, these three security control classes contain 17 control families. Each control family contains security controls related to the security functionality of the family. KPMG included one additional security control class (i.e., program) in its assessment methodology based on a review of NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, and research of relevant security-related statutes, regulations, policies, and guidelines.

Federal security control requirements and assessment methodologies have changed dramatically in recent years in response to new NIST security standards and guidelines. Figure 1 illustrates the relationship of key NIST security standards and guidelines. Appendix I of this report provides additional information about FIPS PUBs and SPs, including their legal effect on the FDIC.

Figure 1: Managing Enterprise Risk (The Framework)



Source: NIST SP 800-53 Rev. 1.

[3] FISMA authorizes the Secretary of Commerce to make NIST standards compulsory for executive agencies to the extent determined necessary to improve the efficiency and security of federal information systems. The Secretary of Commerce exercises this authority subject to the direction of the President and in coordination with the OMB Director. Because the Secretary of Commerce does not have jurisdiction over the FDIC in this subject area, the standards published by the Secretary are not legally binding on the FDIC, but the FDIC's policy is to voluntarily comply with those standards.

[4] Federal agencies must meet the minimum security requirements defined in NIST FIPS PUB 200 through the use of the suggested controls in NIST SP 800-53 Rev. 1. The FDIC has determined that the minimum standards contained in FIPS PUB 200 reflect reasonable business practices that the FDIC should seek to follow.

FDIC Systems and Applications

The FDIC relies extensively on information systems to support its business operations. The FDIC's Division of Information Technology (DIT) maintains seven general support systems (GSS)[6] that provide basic processing and communications support for the 319 business application systems[7] in the Corporation's application inventory. The FDIC's business applications collect, process, store, and distribute mission-critical information, such as personnel and bank data, in support of the Corporation's three primary program areas (Insurance, Supervision and Consumer Protection, and Receivership Management). The FDIC has classified nine of the business application systems as major applications.[8] Table 1 identifies the FDIC's GSSs and major applications. The FDIC has aggregated its minor applications into the GSSs and major applications.

Table 1: The FDIC's General Support Systems and Major Applications

General Support Systems	Mainframe
	Voice/Video
	Mid-range (UNIX) Servers
	Data Communications Infrastructure
	Windows Servers*
	Public Key Infrastructure
	Personal Systems
Major Applications	Assessment Information Management System II
	Asset Servicing Technology Enhancement Program
	Corporate Human Resource Information System
	FDIC*connect*
	Legal Integrated Management System
	New Financial Environment
	Receivership Liability System
	Risk-Related Premium System
	Virtual Supervisory Information on the Net

Source: DIT's Information Security and Privacy Staff.[5]
* During the fiscal year 2007 FISMA evaluation, the FDIC re-defined the boundaries of the Windows Servers GSS to include Windows servers previously included in the Remote Access GSS.

[6] OMB A-130, Appendix III defines a GSS as an interconnected set of information resources under the same direct management and that shares common functionality. A system normally includes hardware, software, information, applications, communications, and people.

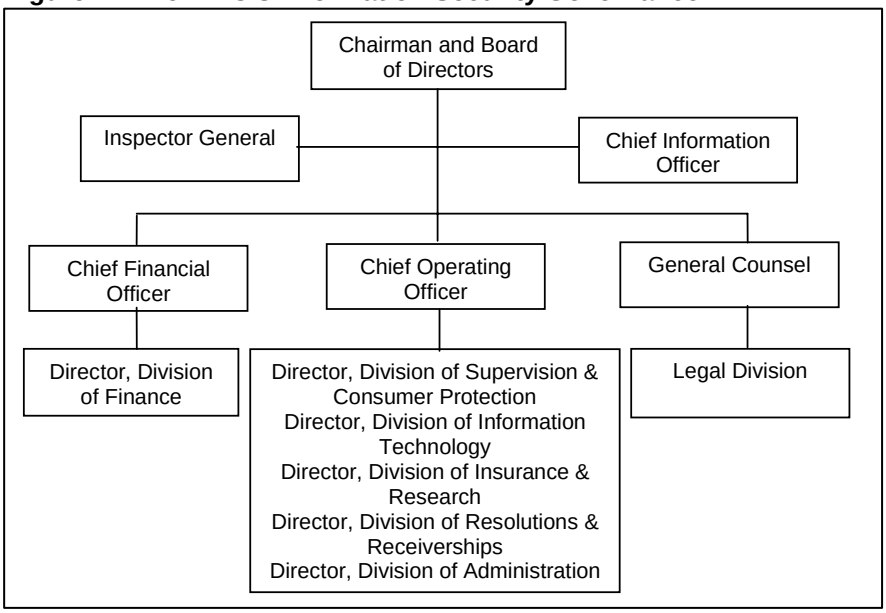
[7] According to the Enterprise Architecture (EA) Repository system inventory of applications systems on July 31, 2007, the FDIC owned 305 application systems and outsourced 14 application systems. Using the July 31, 2007 EA Repository report, DIT Information Security and Privacy Staff (ISPS) identified 152 of the 319 EA Repository application systems inventory and seven GSSs as its risk management inventory subject to FISMA and NIST security requirements. According to the ISPS, the remaining 167 application systems in the EA Repository inventory were no longer in service, or were tools, utilities, or other objects that were not application systems and, therefore, were not included in the ISPS's risk management inventory.

[8] OMB A-130, Appendix III defines a major application as one that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of, the information in the application.

FDIC Security Governance

Several key components comprise the FDIC's information security governance structure. As illustrated in Figure 2, these components include the FDIC Chairman and Board of Directors; Chief Information Officer (CIO); Chief Operating Officer (COO); Chief Financial Officer (CFO); and the Directors of DIT, the Division of Administration (DOA), and other divisions and offices that own information systems.

Figure 2: The FDIC's Information Security Governance



Source: OIG Audit Report No. 06-022, *Independent Evaluation of the FDIC's Information Security Program—2006*, dated September 2006.

The Chairman and Board of Directors are ultimately responsible for the security of the FDIC's information and information systems. The CFO and CIO co-chair a Capital Investment Review Committee, which authorizes and monitors capital projects, including IT projects. The CIO has overall responsibility for the FDIC's IT program, including information security. The CIO also serves as the FDIC's Chief Privacy Officer, Senior Agency Official for Privacy,[9] and Director of DIT. In addition, a CIO Council composed of senior agency managers advises the CIO on all aspects of IT, including security. The COO manages the FDIC's operating divisions, including DIT and DOA. DIT is responsible for providing a secure IT infrastructure and systems. DOA is responsible for providing physical and personnel security for the FDIC. Other division and office heads are responsible for ensuring that systems under their ownership or control conform to the FDIC's security requirements. The OIG performs or contracts for audits and evaluations of the FDIC's information security controls, including the annual independent evaluation of the Corporation's security program required by FISMA.

The CIO has assigned primary responsibility for planning, developing, and implementing the FDIC's information security program and operations to an Associate Director in DIT who reports directly to the CIO. In addition, the FDIC has established eight Information Security Managers (ISM) within its program divisions and offices to ensure a business focus on information security. The responsibilities of ISMs include promoting security awareness, providing security management and technical advice on behalf of their divisions and offices, and assessing the level of security needed and in place in corporate applications. DIT's budget for calendar year 2007 is approximately $191 million, of which the FDIC estimated approximately $18 million is allocated to information security.

[9] The position of Senior Agency Official for Privacy arose from OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, whereas the Chief Privacy Officer resulted from section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, which is Division H of the Consolidated Appropriations Act, 2005. The FDIC determined that the Corporation would comply with these provisions.

DOA's Security and Emergency Preparedness Section is responsible for administering the FDIC's physical and personnel security programs. Physical security includes activities such as badging employees, contractors, and visitors and protecting employees, visitors, and facilities from internal and external threats such as fire, theft, vandalism, sabotage, and terrorist activities. Personnel security includes activities such as performing credit checks, fingerprint checks, and background investigations of FDIC employees and contractors. The Security and Emergency Preparedness Section is also responsible for managing, directing, and testing the FDIC's Emergency Preparedness Program, which includes the FDIC's Emergency Response Plan and the Business Continuity Plan (BCP). Both plans have IT-related components. DIT and DOA coordinate on relevant corporate security matters.

Information Security Program Initiatives

The FDIC is working to implement a number of important initiatives to strengthen its information security program controls and operations. Of particular note, DIT is in the process of deploying software that automatically encrypts data stored on corporate laptop computers without manual intervention by users. The FDIC's current laptop encryption software requires manual intervention by users, limiting management's assurance that sensitive information is consistently encrypted. Additionally, DIT plans to implement a standardized encryption solution for sensitive data stored on removable media, such as Universal Serial Bus (USB) thumb drives and CDs/DVDs. In the fall of 2006, the FDIC undertook a multi-year, strategic initiative to conduct a comprehensive assessment (including usage level, continued need, data content, access rights, and access control monitoring procedures) of its network shared drives. The FDIC recognizes that its network shared drives contain significant amounts of sensitive information that may be at risk of unauthorized disclosure. In addition, DIT initiated the Identity Access Management project to develop a more efficient and effective process for controlling access to its corporate systems and data resources. Further, DIT is adopting the principles of the Control Objectives for Information and related Technology (COBIT®)[10] in its internal control program.

[10] COBIT® is an international IT controls governance framework.

RESULTS OF EVALUATION

The FDIC has made significant progress in recent years in addressing the information security provisions of FISMA and NIST. This progress is noteworthy given the considerable increase in information-security-related requirements levied on federal agencies. KPMG found that the FDIC established policies and procedures in substantially all of the security control areas evaluated. In addition, KPMG noted particular program strength in the areas of *Information Security Governance*, *Incident Response*, and *Awareness and Training*. KPMG also noted that a recent test of the FDIC's IT disaster recovery capability was successful in achieving its primary objective of recovering mission-critical applications and GSSs within pre-determined timeframes. Further, the FDIC enhanced its configuration management controls by integrating information security into its Rational Unified Process (RUP®) systems development life cycle (SDLC) methodology and applying RUP® to IT infrastructure projects.

These accomplishments are notable. However, KPMG identified a number of information security control deficiencies warranting management attention. Addressing these security control deficiencies will contribute to the FDIC's ongoing efforts to achieve reasonable assurance of adequate security over corporate information resources. If not addressed in a timely manner, these security control deficiencies could affect the results of future evaluations of the FDIC's information security program. KPMG's report identifies steps that the Corporation can take to strengthen security controls in *Access Control*; *Identification and Authentication; Risk Assessments*; *Personnel Security*; *Audit and Accountability;* and *Certification, Accreditation, and Security Assessments*. In many cases, the FDIC was already working to improve security controls in these areas during KPMG's evaluation.

Table 2, on the following page, summarizes KPMG's security program assessment results. The table structures KPMG's results according to the security control framework defined in FIPS PUB 200 and SP 800-53 Rev. 1. The table includes one additional control class (i.e., program) based on the results of KPMG's research of relevant security-related statutes, regulations, policies, and guidelines.[11] The detailed results of KPMG's program assessment are presented after Table 2.

[11] Consistent with the FISMA provision that the annual evaluation can be based on a subset of agency systems, KPMG did not assess the *System and Communications Protection* or *Systems and Services Acquisition* control families defined in FIPS PUB 200 and SP 800-53 Rev. 1. Further, KPMG did not assess the *Capital Planning* control family under the Program Controls class. Appendix II describes the security control testing KPMG performed within each security control class and family.

Table 2: KPMG Assessment of the FDIC's Security Controls

Control Class	Control Families Tested That Demonstrated Effectiveness	Control Families Tested That Warrant Management Attention
Program	• Information Security Governance	• Enterprise Architecture
Management	• Planning	• Risk Assessment • Certification, Accreditation, and Security Assessments
Operational	• Contingency Planning • Configuration Management • Maintenance • Incident Response • Awareness and Training	• Physical and Environmental Protection • Personnel Security • System and Information Integrity • Media Protection
Technical	None	• Identification and Authentication • Access Control • Audit and Accountability

Source: 2007 KPMG Evaluation of the FDIC's Information Security Program.

PROGRAM CONTROLS

Program controls define an enterprise-wide framework for planning, directing, and controlling resources to achieve agency security objectives. Based on our analysis of NIST SP 800-100 and relevant security-related statutes, regulations, policies, standards, and guidelines, program controls include three families for consideration: *Information Security Governance, Capital Planning,* and *Enterprise Architecture*. As part of the 2006 FISMA evaluation, the OIG performed extensive testing in these three areas. For 2007, KPMG's evaluation of program controls was limited to *Information Security Governance* and the system inventory component of *Enterprise Architecture*. KPMG did not evaluate security controls related to *Capital Planning*. In summary, KPMG found the security controls tested related to *Information Security Governance* were effective, while controls tested for *Enterprise Architecture* warranted management attention.

Information Security Governance

Rating: Demonstrated Effectiveness

Information security governance involves the implementation of an enterprise-wide control structure that provides management with reasonable assurance that security controls are implemented as designed and operating effectively. Governance consists of (a) enterprise-wide security program policies and procedures that define key roles and responsibilities and (b) monitoring to assess whether security controls are achieving intended results. FISMA defines specific responsibilities and authorities for agency heads,[12] senior agency officials, and CIOs. Among those responsibilities are requirements for the CIO to develop and maintain an information security program and to report annually to the agency head on the effectiveness of the program and progress of remedial actions.

The FDIC has appointed a permanent CIO with corporate accountability and authority for information security, a senior agency information security officer who reports directly to the CIO, and a CIO Council composed of senior agency managers who advise the CIO on all aspects of IT. The FDIC has established a number of policies, procedures, and guidelines that generally define the security roles and responsibilities of corporate officials and contractor personnel. In addition, DIT published an *Information Security Strategic Plan,* and the CIO made periodic presentations to senior agency officials on corporate information security matters. Further, DIT is embracing the principles of COBIT® in its internal control program.

DIT has established a performance measurement program with a current policy, reporting requirements, and a balanced scorecard.[13] Overall, the performance measurement program is maturing, as evidenced by the addition of new performance metrics and retirement of less useful metrics. Currently, there are new metrics under development to better align DIT activities with the Corporation's strategic initiatives. In 2008, DIT plans to include significant updates to its performance metrics. DIT could enhance the utility

[12] For the purposes of our evaluation, we consider the FDIC's Chairman to be the head of the Corporation. Nevertheless, the FDIC's Board of Directors, by statute, has overall responsibility for managing the Corporation. The Board consists of five members: the Chairman, the Vice Chairman, an appointed Director, the Director of the Office of Thrift Supervision, and the Comptroller of the Currency.

[13] The balanced scorecard is a management tool designed to help organizations translate strategy into operational objectives that drive both behavior and performance. The scorecard was designed to improve current performance measurement systems by providing alternatives to managing organizational performance other than exclusively through financial measures.

of the quarterly performance measures and the DIT balanced scorecard by automating the data collection and posting of performance results such that DIT managers could take corrective action more quickly when warranted. Currently, there is an 8- to-10-week time lag between the quarter end and the internal posting of performance results.

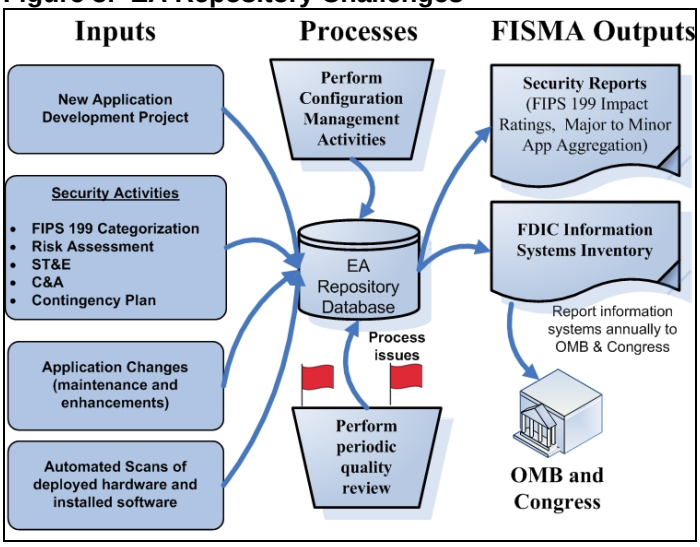
Enterprise Architecture (EA)

Rating: Warrants Management Attention

In business and technological terms, an EA defines an organization's current and target operating environments, including its information security architecture. Effectively representing security information in an EA ensures that security is adequately incorporated into agency system life cycle processes, as required by FISMA. In addition, FISMA requires agencies to develop and maintain an inventory of major information systems, which is a fundamental component of an agency EA.

The FDIC has taken a number of important steps toward full implementation of a corporate-wide EA. Of particular note, the FDIC has established an EA policy and EA governance structure, adopted a SDLC methodology,[14] and developed an EA Repository to store, classify, and organize its EA data (including security data). The FDIC's EA Repository is the inventory of FDIC applications and tools.

Figure 3: EA Repository Challenges



Source: KPMG Analysis.

In July 2007, the FDIC released an improved EA Repository that incorporates enhancements to permit the tracking of various security-related data elements and facilitates the tracking of major and minor applications. However, the FDIC has not assigned responsibility, in writing, for DIT managers or business owners to periodically (quarterly or semi-annually) review the contents of the EA Repository to ensure that it is accurate and reflects events such as system retirements, application upgrades or consolidations, and changes in application points of contact. According to DIT's ISPS, 19 of the 319 application systems in the EA Repository were no longer in use at the FDIC as of July 31, 2007. The lack of data integrity in the EA Repository introduces proved inefficiencies by requiring the use of alternate sources to obtain accurate information, as noted in Figure 3 above. Developing guidance, establishing review procedures, and assigning responsibility will help improve data integrity, promote greater use of the EA Repository in DIT, and reduce reconciliation efforts to prepare a FISMA inventory summary for OMB reporting purposes.

The FDIC retired Circular 1320.3, *Systems Development Life Cycle (SDLC),* and replaced it with DIT Policy 07-005, *Systems Development Life Cycle.* At the time of our evaluation, DIT was working to update Circular 1303.1, *FDIC Enterprise Architecture Program,* dated November 7, 2003, to reflect the

[14] The FDIC's RUP® SDLC methodology includes FDIC-specific security requirements applicable to each phase of the development of an IT project.

current roles and responsibilities and coordination among organizational entities involved with the FDIC's Enterprise Architecture program. The OIG's 2006 security evaluation report required by FISMA noted that Circular 1303.1 was out of date.

MANAGEMENT CONTROLS

Management controls are the safeguards or countermeasures related to an information system that focus on the management of risk and system security. NIST SP 800-53 Rev. 1 divides management controls into four control families: *Risk Assessment*; *Planning*; *System and Services Acquisition*; and *Certification, Accreditation, and Security Assessments*. In summary, security controls tested related to *Planning* were effective. However, controls tested related to *Risk Assessment* and *Certification, Accreditation, and Security Assessments* warranted management attention. We did not evaluate controls related to *System and Services Acquisition.*

Risk Assessment (RA)

Rating: Warrants Management Attention

Risk is the probability of an adverse event occurring. Risk assessment involves the implementation of policies and procedures for categorizing information and systems, performing and updating risk assessments, and performing regular system vulnerability scanning. Risk assessments occur in the system life cycle during the information system's initial development, after significant upgrades, and after the completion of a Security Test & Evaluation (ST&E).[15]

Table 3: Risk Assessment

RA-1	Risk Assessment Policies and Procedures	✓
RA-2	Security Categorization	✓
RA-3	Risk Assessment	✓
RA-4	Risk Assessment Update	✓
RA-5	Vulnerability Scanning	✓

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

Additionally, conducting a risk assessment provides the agency with insight as to whether the security controls in place adequately mitigate threats to the confidentiality, integrity, and availability of the information processed by the system. Further, a current and complete risk assessment satisfies a control requirement of the certification and accreditation (C&A) process as outlined in NIST SP 800-53 Rev.1 and SP 800-37. Under FISMA, agencies are responsible for (a) providing security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems; and (b) establishing policies and procedures that ensure information security is addressed throughout the life cycle of each agency information system.

KPMG identified deficiencies in the FDIC's monthly vulnerability scanning process that prevented some Internet-facing servers and other network equipment from being scanned on a monthly basis. Monthly vulnerability scanning is a key control to identify missing security patches and configuration errors on servers and other network equipment. The OIG recommended in its draft audit report, *FDIC's IT Disaster Recovery Capability*, further enhancements to the FDIC's vulnerability scanning process to ensure all IT devices connected to the network are scanned on a monthly basis. The FDIC initiated corrective actions before that audit's closure.

The FDIC has policies and procedures in place for performing risk assessments for information systems that are generally consistent with NIST guidelines. In addition, DIT leverages an automated risk assessment tool that incorporates the NIST SP 800-53 Rev. 1 control families to identify potential vulnerabilities and countermeasures. However, KPMG observed that the risk assessments for two

[15] ST&E is an examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

selected GSSs, the Windows Servers GSS and Personal Systems GSS, were not updated in the previous three years, or when a significant change occurred to the system, as prescribed by FDIC policy and recommended in NIST guidelines.[16] In the three years following the most recent risk assessments for these systems, significant changes occurred in the FDIC's Windows server environment. Specifically, DIT upgraded approximately one-half of the FDIC's Windows servers (285 out of 596 servers) from Windows 2000 and Windows NT 4.0 operating systems to Windows 2003 operating system. In addition, DIT aggregated the boundaries of the Windows Servers GSS to include 87 FDIC-defined minor applications and contractor systems. DIT's ISPS acknowledged that the risk assessments for these systems had not been updated but explained that full ST&Es for both GSSs had been conducted in the previous two years as well as annual security self-assessments. ISPS concluded that the ST&Es and self-assessments satisfied the intent of NIST's risk assessment guidance.

However, risk assessments identify the controls necessary for adequate security, while ST&Es test the effectiveness of security controls. Accordingly, KPMG believes that DIT should update risk assessments as part of a continuous process that incorporates the outcomes of the ST&Es as recommended by NIST risk management guidance.[17] For example, control deficiencies identified from ST&Es should be subsequently incorporated into risk assessments to retain lessons learned from past control assessments. Where security exposures exist, the risk assessment should suggest additional or compensating controls to mitigate risk. Updates to the risk assessment and identification of additional or compensating controls are subsequently incorporated into System Security Plans (SSPs) and then tested as part of the ST&E.

Planning (PL)

Rating: Demonstrated Effectiveness

Planning involves the implementation of policies, procedures, and practices for developing SSPs. Security plans provide an overview of system security requirements and describe the security controls in place or planned for meeting those requirements. Planning also involves establishing rules that describe user responsibilities and expected behavior related to system usage, as well as conducting system Privacy Impact Assessments (PIA).[18]

Table 4: Planning

PL-1	Security Planning Policy and Procedures	✓
PL-2	System Security Plan	✓
PL-3	System Security Plan Update	✓
PL-4	Rules of Behavior	
PL-5	Privacy Impact Assessment	✓
PL-6	Security-Related Activity Planning	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security control for KPMG testing

The FDIC's security planning policies and procedures were generally consistent with NIST security standards and guidelines. Following the OIG's 2006 FISMA evaluation, the FDIC strengthened its security planning controls by establishing policy and procedures requiring application owners to maintain security plans in StarTeam[19] and to update the SSPs, as part of the SDLC process. However, guidance for preparing SSPs should be enhanced to require that

[16] NIST SP 800-37 states that information system risk assessments are to be performed every three years or whenever there is a significant change to the system or its operational environment.

[17] NIST SP 800-30, *Risk Management Guide for Information Technology Systems* and NIST SP 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*.

[18] PIAs are required under the E-Government Act of 2002 as implemented by OMB's September 26, 2003 Memorandum (M-03-22) entitled, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.

[19] StarTeam is a repository of documents and software source code that permits the FDIC to perform version control and track revision history.

security plans describe how common security controls[20] are considered in the security C&A process, as noted in the 2006 FISMA evaluation. ST&Es of common security controls are performed separately from ST&Es of application and GSS security controls. Enhancing guidance for preparing SSPs would provide greater assurance that all relevant risks identified from the common controls ST&Es are considered when accrediting an application or system.

Following the OIG's 2006 FISMA evaluation, the FDIC strengthened controls in the *Planning* family by enhancing its Security Plan template to incorporate the NIST SP 800-53 Rev. 1 control families. The FDIC also aligned its minor applications with its GSSs and major applications. The FDIC performed this realignment to increase efficiency, identify shared common controls, and incorporate refinements from NIST SP 800-53 Rev. 1. Further, in the OIG's Audit Report No. AUD-07-013, *Response to Privacy Program Information Request in OMB's Fiscal Year 2007 Reporting Instructions for FISMA and Agency Privacy Management*, the OIG concluded that the FDIC's PIA process was satisfactory and consistent with relevant privacy-related policy, guidance, and standards.

System and Services Acquisition (SA)

Rating: Not Evaluated

System and services acquisition involves allocating resources to protect information systems, implementing an SDLC methodology that addresses security, and including security requirements and/or specifications in systems acquisitions. System and services acquisition also includes controls for system documentation, software usage restrictions, security engineering principles, configuration management, and developing security testing during development projects. KPMG did not perform sufficient testing to assess system and services acquisition. The OIG may evaluate system and services acquisition security controls in future FISMA evaluations.

[20] Common security controls can be applied to one or more information systems. Examples of common security controls include controls in *Personnel Security, Incident Response, Physical and Environmental Protection*, and *Contingency Planning*.

Certification, Accreditation, and Security Assessments (CA)

Rating: Warrants Management Attention

The certification and accreditation of federal information systems is critical to securing the government's operations and assets. Certification involves the evaluation of an information system's management, operational, and technical security controls. Accreditation involves a senior agency official's authorization of an information system to operate. OMB requires agencies to certify and accredit their information systems in accordance with federal security policies, standards, and guidelines. At the close of KPMG's current year evaluation, the FDIC reported that it had fully certified and accredited its major applications and GSSs.

Table 5: Certification, Accreditation, and Security Assessments

CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	✓
CA-2	Security Assessments	
CA-3	Information System Connections	
CA-4	Security Certification	✓
CA-5	Plan of Action and Milestones	✓
CA-6	Security Accreditation	✓
CA-7	Continuous Monitoring	✓

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

The FDIC's certification, accreditation, and security assessment policies and procedures were generally consistent with NIST security standards and guidance. However, the FDIC needed to enhance its ongoing security control assessments of its information systems to provide greater assurance that controls are operating effectively. Such enhancements could include, for example, expanding the testing of minor applications, contractor systems, and IT computer services (e.g., Structured Query Language (SQL) database server, Exchange e-mail server). Such enhancements would allow the FDIC to identify and correct the types of operational and technical control deficiencies discussed in this report. Such deficiencies include weak password controls over application and database accounts with access to sensitive information, including PII; sensitive network applications with excessive access privileges; insufficient application audit logging and monitoring; and inadequately secured audit logs.

In the prior three OIG FISMA reports to OMB and the Congress, the OIG had suggested that DIT modify its Plans of Action and Milestones (POA&M) procedures to ensure that all relevant information security deficiencies are incorporated into or accompany system-level POA&Ms. Previously, the FDIC used various systems to track and report system-level security deficiencies based on how the deficiency was identified. For example, system-level security deficiencies identified during the ST&E process were tracked and reported through system-level POA&Ms, while system-level security deficiencies identified during GAO, OIG, and others' reviews were tracked in the Internal Risks Information System (IRIS).[21] In June 2007, the ISPS modified its POA&M practices by developing a POA&M template and process to capture control deficiencies identified by other security reviews beyond the ST&E. ISPS has informed the FDIC's ISMs that POA&Ms should include findings from risk assessments, technical security assessments, ST&Es, FISMA self-assessments, and FDIC OIG or GAO audit findings. KPMG applauds DIT's decision to centralize and consolidate the tracking of information security deficiencies, as this approach is consistent with NIST and OMB guidance.

[21] IRIS is the FDIC's official tracking database for all GAO and FDIC OIG audits and reviews. It is used to track audit findings/conditions, recommendations, and corrective actions/milestones. FDIC divisions and offices can also use IRIS to track the results of their internal control reviews, visitations, and other activities related to managing risks.

While DIT's revised approach for tracking information security vulnerabilities is positive, continued management attention is necessary to ensure the POA&Ms include all known information security deficiencies. During fieldwork, KPMG observed two instances where information security deficiencies were not subsequently incorporated into system-level POA&Ms. In one instance, DIT's information security contractor identified security deficiencies associated with *System and Information Integrity* security control, *SI-2 Flaw Remediation,* that was not incorporated into the Windows Servers POA&M. In another instance, previously reported security deficiencies associated with session time out for inactive remote network connections were not captured in the Windows Servers or Data Communications Infrastructure POA&M. Continued management attention on incorporating all known information security deficiencies into POA&Ms will enable management to better prioritize remediation efforts and track issues through closure.

OPERATIONAL CONTROLS

Operational controls are the safeguards and countermeasures for an information system that are primarily implemented and executed by individuals (as opposed to information systems). Operational controls include nine control families: *Physical and Environmental Protection*; *Personnel Security*; *Contingency Planning*; *Configuration Management*; *Maintenance*; *System and Information Integrity; Media Protection*; *Incident Response*; and *Awareness and Training*. In summary, the controls tested in the areas of *Contingency Planning, Maintenance, Incident Response*, *Configuration Management* and *Awareness and Training* were effective. However, the controls tested related to *Physical and Environmental Protection, Personnel Security, System and Information Integrity*, and *Media Protection* warranted management attention.

Physical and Environmental Protection (PE)

Rating: Warrants Management Attention

Physical and environmental protection relates to those security measures aimed at safeguarding information systems, facilities, and related supporting infrastructures from threats. Such security measures include, but are not limited to, physical access controls, emergency power and lighting, fire protection, and temperature and humidity controls. Such measures also include procedures for the delivery and removal of systems hardware, firmware, and software to and from facilities.

The FDIC has established corporate-wide physical security program policies[22] and procedures. In addition, DIT has conducted security tests and evaluations of *Physical and Environmental Protection* controls and developed POA&Ms to address the control deficiencies it identified. Further, DOA maintained physical access logs for the Virginia Square Data Center. Additionally, DOA enhanced controls over visitors to the FDIC's headquarters facilities by adopting procedures in February 2007 that ensure the verification of visitors' backgrounds and intended purposes before allowing their entry. Such actions were positive; however, during the evaluation, the OIG identified several physical security control deficiencies warranting management attention.

Table 6: Physical and Environmental Protection

PE-1	Physical Security and Environmental Policy and Procedures	✓
PE-2	Physical Access Authorizations	✓
PE-3	Physical Access Control	✓
PE-4	Access Control for Transmission Medium	
PE-5	Access Control for Display Medium	
PE-6	Monitoring Physical Access	✓
PE-7	Visitor Control	✓
PE-8	Access Records	✓
PE-9	Power Equipment and Cabling	
PE-10	Emergency Shutoff	
PE-11	Emergency Power	
PE-12	Emergency Lighting	
PE-13	Fire Protection	
PE-14	Temperature and Humidity Controls	
PE-15	Water Damage Protection	
PE-16	Delivery and Removal	
PE-17	Alternate Work Site	
PE-18	Location of Information System Components	
PE-19	Information Leakage	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓Selected security controls for OIG testing

On July 3, 2007, the OIG conducted an after-hours walkthrough of the FDIC's Virginia Square facility in Arlington, Virginia, and identified one exterior

[22] Such policies include Circulars 1610.1, *FDIC Physical Security Program*; and 1600.2, *FDIC Security in the Workplace Program*.

door to the building and several interior doors to the mainframe and server computer rooms that were unsecured. The doors had been automatically unlocked during our walkthrough by the building's emergency system in response to a water leak in the fire suppression system. However, for several hours, building security personnel were unaware that these doors remained unsecured. Such a vulnerability presented a risk that unauthorized individuals could enter the Virginia Square facility or access sensitive computing areas. An OIG representative notified building security personnel of the vulnerable doors, and guards were subsequently placed at the doors until they were locked. OIG representatives discussed this physical access control vulnerability with DOA officials. DOA subsequently improved procedures for restoring physical access security at the Virginia Square facility following an emergency.

The OIG also identified four unsecured mechanical rooms housing the Virginia Square facility's heating, ventilation, and air conditioning systems, water supply, and electrical equipment. After bringing this matter to DOA's attention, DOA officials determined that the mechanical room doors were not closing properly for various reasons, such as internal airflow pressure on the doors and improper sealing around the doorframes. Prior to the close of our fieldwork, DOA adjusted all four mechanical room doors to ensure they properly close and lock. In addition, during a June 20, 2007 after-hours walkthrough, the OIG identified an unsecured engineering room in the FDIC's main headquarters building housing critical electrical equipment. After alerting the building's security personnel to this vulnerability, the engineering room was locked.

The *Physical and Environmental Protection* control family also includes controls for authorizing physical access to facilities. The OIG was unable to determine whether selected employees recently hired by the FDIC with access to the FDIC's facilities had an appropriate access authorization because access authorization documentation was not readily available. Using a non-statistical sample[23] of 20 employees hired by the FDIC from July 1, 2006 through April 30, 2007, the OIG attempted to verify whether FDIC Form 1620/01, *Employee/Contractor Identification Card Request* (or equivalent documentation), had been completed and approved.[24] DOA officials were unable to locate a completed FDIC Form 1620/01 for seven of the 20 selected employees. The OIG cited a lack of completed FDIC Forms 1620/01 as a deficiency in its 2006 FISMA evaluation report. In response to the OIG's findings, DOA decided to document the authorization and approval of FDIC-issued identification badges for employees already on-board in conjunction with the issuance of new personal identity verification cards that implement Homeland Security Presidential Directive/Hspd-12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD-12).[25] FDIC Forms 1620/01 would continue to be completed whenever new identification cards are issued. However, based on the OIG's current year work, DOA needs to implement additional measures to ensure that FDIC Forms 1620/01 are maintained when new identification cards are issued.

[23] Within this report, we used non-statistical samples and duly noted their use. The results of non-statistical samples cannot be projected to the intended population by standard statistical methods.

[24] FDIC Circular 1610.1, *FDIC Physical Security Program*, states that administrative officers are responsible for approving FDIC Form 1620/01 for all new employees, interns, detailees, and others who require an FDIC identification badge. Once completed and approved, the form is provided to DOA's Corporate Services Branch.

[25] On August 27, 2004, the President issued HSPD-12 requiring the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification. The FDIC is not required to implement HSPD-12, but has decided to voluntarily comply with HSPD-12.

Personnel Security (PS)

Rating: Warrants Management Attention

Personnel security involves the implementation of policies, procedures, and practices for assigning risk designations to positions, screening individuals for those positions, and ensuring that systems access is terminated when personnel leave an agency or are transferred. Personnel security also involves ensuring that appropriate access agreements, such as nondisclosure and conflict of interest agreements, are in place for employees and contractors and implementing a formal sanctions process for personnel who fail to comply with security policies and procedures.

Table 7: Personnel Security

PS-1	Personnel Security Policy and Procedures	✓
PS-2	Position Categorization	✓
PS-3	Personnel Screening	✓
PS-4	Personnel Termination	✓
PS-5	Personnel Transfer	✓
PS-6	Access Agreements	✓
PS-7	Third-Party Personnel Security	✓
PS-8	Personnel Sanctions	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for OIG testing

The FDIC has established personnel-related (employees and contractors) policies, procedures, and guidelines[26] that are generally consistent with NIST guidelines. In addition, the OIG noted that employees and contractors were preparing written confidentiality agreements as prescribed by Circular 2410.1 and the FDIC's *Acquisition Policy Manual*.[27] Further, DIT was in the process of validating its employee position descriptions against actual duties and responsibilities in response to the division's recent re-organization. DIT plans to re-evaluate the appropriateness of its employee risk level designations after it completes ongoing efforts to validate its employee position descriptions. These actions were positive; however, as discussed below, the OIG identified *Personnel Security*-related control deficiencies warranting management's attention.

The OIG reviewed background investigation documentation for employees and contractors to determine whether individuals with physical access to the Virginia Square mainframe or server computer rooms had a background investigation commensurate with the risk associated with their access. FDIC and contractor employees working in FDIC offices undergo a fingerprint and credit check before they are allowed access to FDIC facilities. After an individual begins work, the FDIC and the individual send additional personal information to OPM for a background investigation. Of the 185 individuals who, as of July 13, 2007, had physical access to the mainframe or server computer rooms, 33 did not have OPM background investigations commensurate with the risk associated with their access because the scope of their OPM investigation was below the Moderate risk level. All 33 individuals were DOA contractor employees assigned to contracts that had a risk level designation of Low. Further, the OIG noted that the FDIC had not initiated a background investigation with OPM for six of the 33 referenced individuals and that one of the six individuals had worked for the FDIC for over two years. The FDIC should evaluate the risk level designations of contractor employees with physical access to restricted areas, such as the computer rooms, and allow access only after confirming that OPM has sufficient information to conduct the appropriate background investigation. The OIG briefed DOA management on this condition during the evaluation and identified the individual contractor employees for DOA's review. DOA started the OPM background

[26] Such policies include Circulars 2120.1, *Personnel Suitability Program*; 2210.1, *FDIC Position Management and Classification Program;* 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees*; and 2410.1, *Public and Confidential Financial Disclosure Report and Other Related Employee Ethics Forms Required to be Filed*.

[27] Based on an OIG review of a non-statistical sample of 20 employees hired by the FDIC from July 1, 2006 through April 30, 2007 and 18 security contractor employees at the regional offices the OIG visited.

investigation process for the six contractor employees without an OPM background investigation and is reviewing the duties and risk level designations for the 33 contractor employees.

Using information in the Corporate Human Resources Information System (CHRIS),[28] the OIG selected a separate non-statistical sample of 197 of the FDIC's 4,658 employees on board as of July 19, 2007 to determine whether background investigations were commensurate with risk level designations. As shown in Table 8, the OIG found that 32 employees in positions with a Moderate risk level designation had a background investigation consistent with a Low risk level position. According to a DOA representative, for employees with a High and National Security risk level designation in CHRIS, DOA performed monthly, manual reviews of completed background investigations to identify discrepancies. However, a similar review is not performed for employees with a Moderate risk level designation because of the large number of employees in this category. DOA should develop procedures to better ensure that employee background investigations are commensurate with risk level designations. We discussed this issue with DOA during the evaluation, and DOA began a review of the 32 employees' risk level designations and background investigations.

Table 8: FDIC Employee Risk Level Designations

CHRIS Risk Level Designation	Number of Employees	Number of Employees Sampled	Insufficient Background Investigation
National Security*	63	3	
High	348	29	
Moderate	2,856	161	32
Low	1,391	4	
Totals	**4,658**	**197**	**32**

Source: OIG analysis of CHRIS and DOA records.
* National Security clearance levels are Secret and Top Secret.

DOA recognizes that improvements are needed in its processes for establishing risk level designations and conducting background investigations. In a September 29, 2006 internal report, DOA's Management Support Section concluded that audit trails for approving, authorizing, verifying, reconciling, and maintaining risk level designation determinations within DOA were not clearly evident as changes are made. The report also noted that supporting documentation was often not retained or did not exist to support risk level determinations or changes in risk level assignments within DOA. DOA was working to address the deficiencies identified in the internal review report during this evaluation.

[28] CHRIS is a major application that provides human resource related information.

Contingency Planning (CP)

Rating: Demonstrated Effectiveness

Effective contingency planning and testing is essential to mitigate the risk of system and service unavailability. Contingency planning involves developing and implementing system contingency plans that address roles, responsibilities, and activities associated with restoring a system after a disruption or failure. Such planning also involves training personnel, testing systems, performing system backups, and establishing alternative processing sites.

Table 9: Contingency Planning

CP-1	Contingency Planning Policy and Procedures	✓
CP-2	Contingency Plan	✓
CP-3	Contingency Training	✓
CP-4	Contingency Plan Testing and Exercises	✓
CP-5	Contingency Plan Update	✓
CP-6	Alternative Storage Sites	✓
CP-7	Alternative Processing Sites	✓
CP-8	Telecommunication Services	✓
CP-9	Information System Backup	✓
CP-10	Information System Recovery and Reconstitution	✓

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

The FDIC has taken a number of positive steps in the area of contingency planning. Of particular note, the FDIC has established a DIT contingency planning program policy.[29] Further, the FDIC has documented system recovery plans in the *DIT Business Continuity Plan* that were current and consistent with NIST guidance. In addition, the FDIC conducted a disaster recovery test of its mission-critical applications and GSSs in April 2007. The disaster recovery test was successful in achieving its primary objective of recovering the FDIC's mission-critical applications and GSSs within pre-determined timeframes. The FDIC prepared a formal report detailing the results of its disaster recovery testing and developed plans to address the issues it identified during the testing.

The above actions are positive; however, a recent audit of the FDIC's IT disaster recovery capability[30] identified several opportunities for the FDIC to improve its Contingency Planning controls. Specifically, the audit noted that DIT needed to update the FDIC's contingency planning program policy to reflect the Corporation's current IT disaster recovery environment and recent NIST guidance, and document (and test as appropriate) its plans for recovering certain security services designed to protect the FDIC's network during a disaster. In addition, the audit noted that the FDIC was working to update its Business Impact Analysis (BIA). Based on the collective control strengths and deficiencies related to contingency planning, KPMG determined that the *Contingency Planning* control family demonstrated effectiveness.

[29] Circular 1360.13, *DIT's Contingency Planning Program Policy*, dated November 22, 2004.
[30] Draft OIG Report, *FDIC's IT Disaster Recovery Capability*, dated August 24, 2007. KPMG provided technical assistance to the FDIC OIG in the evaluation of FDIC's IT Disaster Recovery capability.

Configuration Management (CM)

Rating: Demonstrated Effectiveness

Key to ensuring the confidentiality, integrity, and availability of any information system is implementing structured processes for managing the inevitable changes that will occur during the system's life cycle. Such processes, collectively referred to as configuration management, include evaluating, authorizing, testing, tracking, reporting, and verifying both hardware and software changes. Inadequate configuration management controls increase the risk that unauthorized programs or untested changes could inadvertently or deliberately be implemented and negatively affect system performance or security.

Table 10: Configuration Management

CM-1	Configuration Management Policies and Procedures	✓
CM-2	Baseline Configuration	✓
CM-3	Configuration Change Control	✓
CM-4	Monitoring Configuration Changes	
CM-5	Access Restrictions for Change	✓
CM-6	Configuration Settings	✓
CM-7	Least Functionality	✓
CM-8	Information System Component Inventory	✓

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

Importantly, the FDIC established a corporate-wide software configuration management policy covering all of its application and system software.[31] The policy requires that the FDIC's software configuration management practices be consistent with the principles of the Capability Maturity Model Integration (CMMI)[32] and relevant federal standards and guidelines. In addition, DIT established the *FDIC Infrastructure Change Control Board* to, among other things, review and approve changes to the FDIC's IT infrastructure and technical architecture, including the Windows Servers and Personal Systems GSS. DIT also developed software configuration management plans for its Windows Servers and Personal Systems GSS.

On March 22, 2007, OMB issued Memorandum M-07-11 entitled, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*.[33] The OMB memorandum requires agencies using the Windows XP operating system to adopt the security configurations developed by NIST, the Department of Defense, and the Department of Homeland Security no later than February 1, 2008. The OMB memorandum states that adopting such configurations are important to improving information security and reducing overall IT operating costs. As part of its FISMA evaluation work, KPMG compared the security configuration settings recommended in NIST SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist* (dated October 2005), to the standard security configuration settings of the FDIC's Windows XP desktop. KPMG noted that 27 of 133 configuration settings implemented by the FDIC, including settings related to passwords, account lockouts, and event log sizes, were less restrictive than those recommended in NIST SP 800-68. Implementing configuration settings that are less restrictive than those recommended by NIST can pose additional risks to the confidentiality, integrity, and availability of FDIC desktops and laptops. KPMG brought these discrepancies to DIT's attention during the evaluation, and DIT began evaluating the impact. DIT is currently seeking internal approval of an automated tool that will facilitate a comparison of the security configuration settings of the FDIC's Windows servers and desktops to NIST-recommended configuration settings. As of the time of our fieldwork, DIT planned to implement the tool in September 2007. DIT officials indicated that there were differences between the

[31] Circular 1320.4, *FDIC Software Configuration Management Policy*, dated June 8, 2006.
[32] A process improvement methodology developed by Carnegie Mellon University's Software Engineering Institute.
[33] The FDIC has determined that, in connection with this memorandum, OMB does not have authority to direct the FDIC to take certain actions of OBM's choosing.

configuration settings implemented by the FDIC and those recommended by NIST SP 800-68 because the FDIC had initially adopted a security configuration based on the National Security Agency's guidance prior to the publication of NIST SP 800-68 in October 2005.

Further, KPMG's testing showed that DIT has effective controls in place for monitoring and tracking configuration changes for information systems. KPMG reviewed a non-statistical sample of 30 configurations out of total population of 456 and successfully identified change approvals from DIT for each one.

Maintenance (MA)

Rating: Demonstrated Effectiveness

Maintenance involves scheduling, performing, and documenting preventative and regular maintenance on components of information systems in accordance with manufacturer or vendor specifications and/or organization requirements. Maintenance also involves approving, controlling, and monitoring maintenance tools and activities.

Table 11: Maintenance

MA-1	System Maintenance Policy and Procedures	✓
MA-2	Controlled Maintenance	✓
MA-3	Maintenance Tools	
MA-4	Remote Maintenance	
MA-5	Maintenance Personnel	
MA-6	Timely Maintenance	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

The FDIC has established policies and procedures for maintaining its information system components. Importantly, the FDIC maintains current, vendor-supported operating system software for its Windows servers and Windows desktops and laptops. Further, at the time of our evaluation, the FDIC was in the process of replacing its laptop computers as part of a planned corporate laptop replacement project.

System and Information Integrity (SI)

Rating: Warrants Management Attention

Table 12: System and Information Integrity

SI-1	System and Information Integrity Policy and Procedures	✓
SI-2	Flaw Remediation	✓
SI-3	Malicious Code Protection	✓
SI-4	Information System Monitoring Tools and Techniques	✓
SI-5	Security Alerts and Advisories	
SI-6	Security Functionality Verification	
SI-7	Software and Information Integrity	
SI-8	Spam Protection	
SI-9	Information Input Restrictions	
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	
SI-11	Error Handling	
SI-12	Information Output Handling and Retention	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

System and information integrity includes security controls for identifying, reporting, and correcting information system flaws. Such flaws can be discovered through system security assessments, continuous monitoring, or software vendors that recommend the implementation of software patches, service packs, or hotfixes to their software. System and information integrity also involves the deployment of virus protection and intrusion detection mechanisms to protect the agency's IT operations and the implementation of controls to ensure the accuracy, completeness, and validity of information.

The FDIC has established policies and procedures designed to ensure the integrity of its systems and information. DIT has deployed anti-virus software to protect its Windows Servers and Personal Systems GSS and implemented a new intrusion detection system (IDS) within the last year to log, store, and aggregate network IT events. In addition, DIT has established a software patch management policy,[34] adopted performance measures to monitor the deployment of patches against pre-established timeframes, and reported the status of its patch identification, testing, and deployment activities. DIT has been working hard to ensure the timely implementation of software patches in the Windows Servers and Personal Systems GSSs. However, continued management attention is warranted to ensure that all Windows servers are appropriately patched in a timely manner to protect against known security vulnerabilities.

As part of system and information integrity control testing, KPMG selected 34 of 67 Windows servers in the FDIC's disaster recovery computing facility on April 26, 2007 for a detailed security configuration review. KPMG found that 2 of the 34 servers were each missing over 40 security patches. Many of the missing security patches were classified by the Microsoft Corporation as critical, presenting a serious risk to the operation of the servers. Although DIT took prompt action to patch the two vulnerable servers during the FISMA evaluation, these actions provided only a temporary solution to a broader management challenge. The OIG indicated in a draft report[35] that DIT should implement control improvements in its patch deployment processes to help ensure that all Windows servers are patched in a timely manner. In addition, KPMG noted that limitations in DIT's vulnerability scanning processes prevented DIT from detecting the lack of security patches on these two servers. Accordingly, the OIG is recommending that DIT enhance its vulnerability scanning processes to ensure that all servers in the production environment are routinely scanned for security vulnerabilities.

[34] DIT Policy 04-004, *Policy on Security Patch Management*, published April 15, 2005

[35] Draft OIG Report, *FDIC's IT Disaster Recovery Capability*, dated August 24, 2007. KPMG provided technical assistance to the FDIC OIG in the evaluation of FDIC's IT Disaster Recovery capability.

Media Protection (MP)

Rating: Warrants Management Attention

Media protection involves those security controls related to controlling access to hardcopy and electronic media, labeling media consistent with its sensitivity, and ensuring the security of stored media. Media protection also involves safeguarding the transportation of media and ensuring that appropriate controls are in place when sanitizing and disposing of media.

Table 13: Media Protection

MP-1	Media Protection Policy and Procedures	✓
MP-2	Media Access	
MP-3	Media Labeling	✓
MP-4	Media Storage	✓
MP-5	Media Transport	
MP-6	Media Sanitation and Disposal	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

On April 30, 2007, the FDIC issued Circular 1360.9, *Protecting Sensitive Information*, requiring, among other things, that FDIC employees and contractors label portable storage media (e.g., CDs/DVDs and USB thumb drives) as containing sensitive information; limit access to sensitive information to only those individuals with a business need to know; store sensitive information only on Corporation-owned IT equipment; encrypt sensitive information stored on end-user IT equipment (e.g., FDIC laptop computers) and portable storage media; properly dispose of sensitive electronic media when it is no longer needed; and notify appropriate officials should a compromise of sensitive information occur. The issuance of this policy was a significant improvement for the FDIC's media protection controls. However, as described below, KPMG identified several control areas related to media protection that warranted management attention.

As of August 31, 2007, the FDIC was in the process of deploying new software that automatically encrypts sensitive information stored on the FDIC's laptop computers. This software is replacing the FDIC's older encryption solutions that require manual intervention by users, limiting management's assurance that sensitive information is consistently encrypted. In addition, a recent audit completed by the OIG noted that FDIC employees were not encrypting sensitive information stored on portable storage media as prescribed by FDIC policy.[36] Although the FDIC has implemented encryption software to protect sensitive information stored on portable storage media, the software also requires manual intervention by users, limiting management's assurance that sensitive information is consistently encrypted. DIT plans to identify and subsequently deploy new encryption software for its portable storage media. DIT also plans to deploy encryption software on all agency Personal Digital Assistants and BlackBerrys®.

On June 20 and July 3, 2007, the OIG conducted after-hours walkthroughs of selected FDIC headquarters facilities and identified hardcopy sensitive information (including PII) stored in unsecured filing rooms and unsecured filing cabinets located in common areas. The OIG promptly notified DOA and DIT officials of the locations of this information, and corrective action was taken or underway at the close of our evaluation. The OIG also conducted walkthroughs of three FDIC regional office buildings in June 2007. In general, the OIG found that regional offices were taking reasonable steps to secure sensitive hardcopy information. However, the OIG noted isolated instances of unsecured PII in each of the three regional offices visited. The OIG immediately brought these isolated instances to the attention of regional office officials, and corrective action was taken to secure the hardcopy and electronic media.

[36] FDIC OIG Audit Report No. AUD-07-010, *Division of Resolutions and Receiverships Protection of Electronic Records*, dated September 5, 2007.

The FDIC routinely transports mainframe and server backup tapes to an off-site contactor location for both archiving and disaster recovery purposes. Although the backup tapes contain sensitive information, they are not encrypted. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, recommends that agencies encrypt all data on mobile computers/devices that carry agency data unless the data is determined, in writing, to be non-sensitive data. In addition, NIST SP 800-53 Rev. 1 states that an organization's assessment of risk should guide the use of encryption for backup information. Given the high volume of data stored on its backup tapes, the loss or compromise of a backup tape could have a significant impact on the FDIC. At the close our evaluation, a DIT official advised KPMG that DIT had investigated available encryption solutions for securing tape media but had not found a solution that would operate across its IT environment. The DIT official stated DIT is concentrating its encryption efforts on the higher-risk areas such as laptops, USB thumb drives, Blackberrys®, PDAs, and desktops before exploring encryption for its backup tapes. Although not specifically required by statute, NIST standards, or OMB guidelines, the FDIC should consider encrypting its backup tapes to reduce the risk of a potential unauthorized disclosure of sensitive information

Incident Response (IR)

Rating: Demonstrated Effectiveness

FISMA requires that agency information security programs include procedures for detecting, reporting, and responding to security incidents.[37] Implementing an effective incident response capability involves considering many factors, including training and detection, analysis, containment, eradication, reporting, and recovery from security incidents.

Table 14: Incident Response

IR-1	Incident Response Policy and Procedures	✓
IR-2	Incident Response Training	
IR-3	Incident Response Testing and Exercises	
IR-4	Incident Handling	✓
IR-5	Incident Monitoring	
IR-6	Incident Reporting	✓
IR-7	Incident Response Assistance	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

The FDIC maintains a computer security incident response capability that is consistent with NIST SP 800-61, *Computer Security Incident Handling Guide*. The FDIC has prepared procedural manuals containing detailed guidance for the prevention, detection, analysis, response, recovery, and reporting of security incidents. The FDIC also provides regular training for its Computer Security Incident Response Team members. At the close of our evaluation, DIT was working to develop a security breach plan and guidelines in response to OMB's May 22, 2007 Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

[37] NIST SP 800-61 defines an incident as a violation of computer security policies, acceptable use policies, or standard computer security practices.

Awareness and Training (AT)

Rating: Demonstrated Effectiveness

Table 15: Awareness and Training

AT-1	Security Awareness and Training Policy and Procedures	✓
AT-2	Security Awareness	✓
AT-3	Security Training	✓
AT-4	Security Training Records	✓
AT-5	Contacts with Security Groups and Associations	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓Selected security controls for KPMG testing

FISMA requires federal agencies to provide security awareness training to users of agency information systems and requires agency CIOs to ensure proper oversight and training of personnel with significant information security responsibilities. In addition, federal regulations[38] require agencies to develop a security awareness and training plan, identify employees with significant security responsibilities, and provide role-specific training in accordance with NIST standards and guidelines.

Circular 1360.16, *Mandatory Information Security Awareness Training*, requires users of the FDIC's network to complete an annual Web-based information security awareness orientation.[39] The circular states that new employees shall log on and review the FDIC's information security awareness Web-site and orientation as soon as their network access is granted; failure to do so within 5 working days of receiving a network ID may result in revoking the employee's or contractor's access to FDIC systems and applications. The FDIC continued its prior-year practices of requiring (a) network users to complete the annual security awareness orientation, (b) major application users to complete application-specific security awareness training, and (c) GSS technicians and managers to complete system-specific security training. In addition, DIT developed a formal training plan to ensure its staff with significant information security responsibilities receive appropriate security training for the type of work they perform.

KPMG determined that DIT had addressed a prior-year deficiency related to new network users not completing the security awareness orientation on a timely basis. In addition, KPMG identified several opportunities for DIT to enhance the effectiveness of the FDIC's security awareness and training practices. Such enhancements include, for example, better integration of the FDIC's security policies and procedures. KPMG discussed these minor enhancements during a September 6, 2007 meeting with the CIO.

[38] The FDIC has determined that these regulations entitled, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems* (5 Code of Federal Regulations Part 930 Subpart C) apply to the Corporation.

[39] The orientation includes information about laws, regulations, and policies related to computer security; rules of behavior for systems and major applications; tips on effective security; and links to additional sources of information.

TECHNICAL CONTROLS

Technical controls are the safeguards or countermeasures for an information system that are primarily implemented and executed by the system through mechanisms contained in the hardware, software, or firmware components of the system. NIST SP 800-53 Rev. 1 separates technical controls into four control families: *Identification and Authentication*; *Access Control*; *Audit and Accountability;* and *System and Communications Protection*. In summary, the controls tested related to *Identification and Authentication, Access Control,* and *Audit and Accountability* warranted management attention. We did not evaluate *System and Communications Protection* as part of our current-year work.

Identification and Authentication (IA)

Rating: Warrants Management Attention

Identification and authentication includes security controls designed to verify the identity of individual users, processes, or devices as a prerequisite to allowing access to information systems and data. Identification and authentication can be accomplished using various means, such as passwords, card tokens, biometrics, or some combination thereof.

Table 16: Identification and Authentication

IA-1	Identification and Authentication Policy and Procedures	✓
IA-2	User Identification and Authentication	✓
IA-3	Device Identification and Authentication	
IA-4	Identifier Management	✓
IA-5	Authenticator Management	
IA-6	Authenticator Feedback	✓
IA-7	Cryptographic Module Authentication	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

The FDIC established policies and procedures designed to identify and authenticate users of its information systems. However, KPMG identified security control deficiencies warranting management attention. Specifically, KPMG conducted a limited review of the security configuration of four database servers in the Windows Servers GSS as of July 20, 2007 and identified five database accounts with weak passwords. None of the passwords used to protect these five accounts satisfied the requirements of Circular 1360.10, *Corporate Password Standards*, regarding (among other things) length, use of alphanumeric or special characters, periodic resets, and complexity (i.e., hard to guess). Circular 1360.10 states that passwords must be well designed and properly implemented because they are often the first line of defense for limiting access to corporate data to authorized users. These password deficiencies elevated the risk that a network user could have used these accounts, without authorization, to access, modify, or delete sensitive FDIC information. KPMG apprised DIT of the weak password deficiencies, and DIT promptly took corrective action. DIT should enhance its continuous monitoring program to achieve greater assurance of detecting weak passwords throughout the Windows Servers GSS.

NIST recommends that organizations encrypt passwords when transmitted over a network to guard against eavesdropping. Generally, the FDIC observes this security practice; however, KPMG identified two instances where user IDs and passwords were transmitted without being encrypted across the FDIC's internal network in its data center. In one instance, KPMG noted that the FDIC's Remote Client Network (RCN) Web servers did not encrypt user IDs and passwords that it exchanged with other RCN Windows servers across the FDIC's internal network. In a second instance, KPMG observed that a Windows job-scheduling server exchanged a powerful mainframe user ID and password without encryption to the FDIC's production mainframe to initiate batch jobs. Circular 1360.10, *Corporate Password Standards*,

states that passwords must never be transmitted without being encrypted. KPMG recognizes that mitigating controls, such as physical security controls, exist. However, the FDIC could improve its identification and authentication controls by implementing only those technical solutions that encrypt user IDs and passwords.

FIPS PUB 201, *Personal Identity Verification of Federal Employees and Contractors,* and associated publications establish standards and requirements for the identity verification of federal employees and contractors and for the issuance of Personal Identity Verification (PIV) credentials.[40] OMB directed agencies to begin issuing identity credentials to meet the FIPS PUB 201 standard by October 27, 2006.[41] Government corporations such as the FDIC are encouraged to comply with HSPD-12. With regard to the FDIC's efforts to implement a PIV system that is consistent with FIPS PUB 201 for its employees and contractors, DOA has drafted a project plan describing the FDIC's intended approach for implementing the goals and objectives of HSPD-12. According to the draft plan, the FDIC estimates that it will begin issuing HSPD-12 compliant identity credentials in late 2007 or early 2008.

[40] NIST issued FIPS PUB 201 in response to HSPD-12.

[41] OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,* dated August 5, 2005.

Access Control (AC)

Rating: Warrants Management Attention

Information system access controls (i.e., logical access controls) provide assurance that system resources can be accessed only by authorized users in authorized ways. Logical access controls provide a technical means of controlling the information users can read and copy, the programs they can execute, and the modifications they can make.

Table 17: Access Control

AC-1	Access Control Policy and Procedures	✓
AC-2	Account Management	✓
AC-3	Access Enforcement	✓
AC-4	Information Flow Enforcement	
AC-5	Separation of Duties	✓
AC-6	Least Privilege	✓
AC-7	Unsuccessful Login Attempts	✓
AC-8	System Use Notification	✓
AC-9	Previous Logon Notification	
AC-10	Concurrent Session Control	
AC-11	Session Lock	
AC-12	Session Termination	✓
AC-13	Supervision and Review – Access Control	✓
AC-14	Permitted Actions w/o Identification and Authentication	
AC-15	Automated Marking	
AC-16	Automated Labeling	
AC-17	Remote Access	✓
AC-18	Wireless Access Restriction	
AC-19	Access Control for Portable and Mobile Devices	✓
AC-20	Use of External Information Systems	✓

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

The FDIC has established policies and procedures that communicate corporate-wide roles and responsibilities for managing access to its information systems, data, and remote access.[42] The FDIC was also working to implement several key initiatives aimed at strengthening access controls. Such initiatives include a corporate effort to secure sensitive information stored on the FDIC's internal network shared drives and a project to reengineer and integrate the FDIC's access control systems and procedures. While these actions were positive, KPMG identified deficiencies in the following controls: separation of duties, least privilege, and session termination, as described below.

With regard to separation of duties, KPMG noted that as of July 20, 2007, four FDIC employees and eight contractor personnel were members of a powerful Windows group called the Windows Domain Admins group. Limiting membership in the Windows Domain Admins group based on business need is critical because the group allows its members to grant themselves access to Windows applications and record transactions and to delete application audit logs. Microsoft's publication entitled, *Best Practices for Delegating Active Directory Administration,* recommends that organizations assign only two or three system administrators to the Windows Domain Admins group. The FDIC can promote improved separation of duties in the Windows GSS by evaluating the feasibility of reducing the number of system administrators in the Windows Domain Admins group and by delegating specific administrative activities to less powerful administrative groups, where possible. In this manner, the FDIC can mitigate the risk that system administrators can alter and delete security logs and limit system administrators' ability to alter application data. The FDIC should also evaluate other

[42] Such policies and procedures include, but are not limited to, Circulars 1360.15, *Access Control for Automated Information Systems*; and 1370.1, *Periodic Review of Mainframe Resource Access*; the FDIC's *Access Control Procedures and Guidelines*; and *Information Security Manager's (ISM) Guide*.

Windows administrative groups to ensure that appropriate separation of duties exists. Such an effort could be integrated into the FDIC's Identity and Access Management project.

The security principle of least privilege refers to the practice of restricting user access to only those IT resources, including data, needed to perform official duties. The FDIC did not always restrict access to sensitive information, including PII, on the FDIC's internal network to users with a business need to access the information. As reported in the OIG's Audit Report No. AUD-07-010, *Division of Resolutions and Receiverships Protection of Electronic Records*, access to sensitive resolution and receivership information, including PII, stored on the FDIC's internal network was not adequately protected. FDIC security officials took prompt action to restrict access to the sensitive information identified during the OIG audit; however, during our FISMA evaluation work, KPMG identified additional instances in which sensitive data was stored on internal network shared drives without adequate access restrictions. Further, KPMG tested a non-statistical sample of 67 Windows servers, deemed mission-critical by DIT, and identified eight servers that granted all users full control of 14 network shared drives. One of the 14 network shared drives contained the security event logs for all Windows Servers. Any user on the internal network could read, modify, or delete these critical security logs. This deficiency limited the FDIC's assurance regarding the integrity of the IT security logs. At the close of our evaluation, the FDIC was working to address these issues as part of a broader Corporate initiative.

With regard to security control *AC-12 Session Termination*, the FDIC did not always automatically terminate remote sessions after 30 minutes of inactivity. As stated in OMB memorandum M-06-16, *Protection of Sensitive Agency Information*, remote access sessions should terminate after a period of user inactivity. Time-out functionality testing of the FDIC's four remote access solutions[43] showed several situations where the remote session does not terminate after 30 minutes of inactivity. As a compensating control, DIT has instituted a 15-minute password-protected screensaver on all agency laptops. However, this compensating control does not apply when users remotely access the FDIC network from a non-FDIC (e.g., home) computer.

KPMG identified other access control deficiencies related to Windows server security; however, because these deficiencies were less significant, KPMG communicated them separately to the CIO.

[43] The four remote access solutions are Ascend Dial-in, RCN, FastAccess, and WebVPN.

Audit and Accountability (AU)

Rating: Warrants Management Attention

Audit and Accountability involves generating audit records at a sufficient level of detail to establish the events that took place, sources of the events, and outcomes of the events. *Audit and Accountability* also involves consideration of audit trail storage, processing, monitoring, reporting, protection, and retention. Audit records, together with appropriate tools and procedures, promote key security-related objectives, such as detecting security violations, individual accountability, and reconstructing auditable events. To be effective, agencies should configure their software to collect and maintain audit trails that are sufficient to track security-related events.

Table 18: Audit and Accountability

AU-1	Audit and Accountability Policy and Procedures	✓
AU-2	Auditable Events	✓
AU-3	Contents of Audit Records	✓
AU-4	Audit Storage Capacity	✓
AU-5	Response to Audit Processing Failures	✓
AU-6	Audit Monitoring, Analysis, and Reporting	✓
AU-7	Audit Retention and Report Generation	
AU-8	Time Stamps	✓
AU-9	Protection of Audit Information	✓
AU-10	Non-repudiation	✓
AU-11	Audit Record Retention	

Source: NIST SP 800-53 Rev. 1.
Legend: ✓ Selected security controls for KPMG testing

The FDIC has established policy and procedures to incorporate audit and accountability controls within its information systems. Regarding the control AU-6, *Audit Monitoring, Analysis, and Reporting*, the FDIC's ISMs review and report on access violations for the Windows Servers GSS. Additionally, the FDIC's Computer Security Incident Response Team (CSIRT) monitors the Windows security audit log, a host-based IDS solution, and changes to group membership for selected Windows administrator groups. KPMG's testing verified that a central tracking system tracks the addition and deletion of users within selected administrator groups and that CSIRT initiates appropriate action when warranted.

While these controls are positive, opportunities for improvement remain. Also, in regard to security control AU-6, KPMG observed that DIT did not regularly review or analyze application audit logs within the Windows Servers GSS unless instructed by the system owner. To address this and previously noted deficiencies,[44] the FDIC established a one-year project plan to improve its audit logging and monitoring of FDIC applications. Further, the FDIC developed a draft strategy document to achieve the following objectives:

- establish an enterprise-wide program for audit logging and monitoring,
- develop requirements for the monitoring program,
- standardize the approach for implementing the monitoring function, and
- establish roles and responsibilities for DIT and system owners.

Lastly, DIT drafted policy for logging and monitoring of audit records. While positive steps have been taken, KPMG observed that formal, documented procedures to facilitate the implementation of the audit and accountability controls were not implemented for application and system audit logs. Additionally, as mentioned within the Access Control family, DIT did not provide sufficient protection of audit records from unauthorized access, modification, and deletion.

[44] FDIC OIG Audit Report No. 06-025, *Controls for Monitoring Access to Sensitive Information Processed by FDIC Applications*, dated September 29, 2006.

System and Communications Protection (SC)

Rating: Not Evaluated

System and communication protection addresses a number of key security control objectives, including ensuring that system functionality is appropriately segregated; communications are monitored, controlled, and protected; and cryptographic operations are adequate.

The FDIC has taken a number of steps toward ensuring that all communications paths provide confidentiality, integrity, and availability. Specifically, DIT has provided a means for encrypting all e-mail communication across the network, and DIT has successfully tested and begun deploying laptops with encrypted hard drives.

KPMG did not perform specific audit procedures related to system and communications protection because the majority of controls in this family pertain to GSSs not covered under our current-year evaluation. Such GSSs include the Public Key Infrastructure and Data Communication Infrastructure systems. The OIG may evaluate system and communications protection security controls in future FISMA evaluations.

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the FISMA evaluation was to evaluate the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards, and guidelines. The scope of the FISMA evaluation included the Windows Servers, Remote Access, and Personal Systems GSSs. KPMG limited the scope of the FISMA evaluation within the Remote Access and Personal Systems GSS to the Windows 2000/2003 server components and the Windows XP desktop to assess the FDIC's implementation of provisions in OMB Memorandum M-06-16, *Protection of Sensitive Agency Information.* Other hardware and software components within the Remote Access and Personal Systems GSS were not tested. The scope of the FISMA evaluation also included reviewing the FDIC's common security controls such as *Awareness and Training, Incident Response, Contingency Planning,* and *Personnel Security*. Finally, KPMG reviewed the corrective actions taken to address issues identified during the FY 2006 FISMA evaluation.

To accomplish the evaluation's objective, KPMG reviewed prior-year audit reports, including GAO's report on the FDIC's information security,[45] the OIG's FY 2005 and FY 2006 FISMA evaluations,[46] and various FDIC OIG reports on information security to identify deficiencies and potential risk areas. In addition, KPMG conducted interviews with appropriate FDIC personnel to obtain an understanding of each area within the scope of the evaluation, updates in the control areas covered in prior-year reviews, and the status of any corrective actions. Further, KPMG reviewed FDIC documentation applicable to information security, including FDIC directives and DIT internal policies.

The FISMA evaluation did not assess controls at depository institutions insured or regulated by the FDIC that routinely provide financial information to the Corporation. KPMG performed its FISMA evaluation during the period April through August 2007 at the FDIC's Headquarters offices and primary computer facility in Arlington, Virginia, and its disaster recovery site. Throughout the FISMA evaluation, KPMG met with FDIC management to discuss preliminary conclusions.

The FDIC OIG contracted with KPMG to evaluate the FDIC's compliance with FISMA requirements and report on the FDIC's IT controls over its information security program. KPMG conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards* issued by the Comptroller General of the United States. 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. This performance audit did not constitute an audit of financial statements in accordance with generally accepted government auditing standards. We were not engaged to and did not express an opinion on the FDIC's internal controls over financial reporting or over financial management systems (for purposes of OMB's Circular No. A-127, *Financial Management Systems*, July 23, 1993, as revised). We caution that projecting our evaluation to future periods is subject to the risk that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

[45] *Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program,* GAO-07-351, May 18, 2007; see http://www.gao.gov/new.items/d07351.pdf.

[46] FDIC OIG Audit Report No. 06-022, *Independent Evaluation of the FDIC's Information Security Program– 2006*, dated September 28, 2006 and FDIC OIG Audit Report No. 05-040, *Independent Evaluation of the FDIC's Information Security Program– 2005*, dated September 30, 2005.

Computer-based Data, Performance Measures, and Fraud and Illegal Acts

We performed appropriate procedures to assure ourselves that computer-based data were valid and reliable when those data were significant to our evaluation findings and conclusions. Such procedures included verifying selected automated data to source documentation and corroborating automated data through interviews with appropriate FDIC personnel. Finally, we did not develop specific audit procedures to detect fraud and illegal acts because we did not consider fraud and illegal acts to be material to the evaluation objective. However, throughout our evaluation, we were sensitive to the potential for fraud and illegal acts, and none came to our attention.

Internal Control

An explanation of the terms *internal control*, *reasonable assurance*, and *adequate security* is important to ensure a proper understanding of our approach and conclusions. OMB Circular No. A-123 (OMB A-123), *Management's Responsibility for Internal Control*,[47] states:

> *Internal Control*—organization, policies, and procedures—are tools to help program and financial managers achieve results and safeguard the integrity of their programs.

Additionally, OMB A-123 states that *internal control* must provide reasonable assurance as follows:

> *Internal control* is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

OMB A-130, Appendix III,[48] defines *adequate security* as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or modification of or unauthorized access to information." This includes assuring that agency systems and applications provide appropriate confidentiality, integrity, and availability using cost-effective, risk-based management, personnel, operational, and technical controls. The concept of *adequate security* is consistent with FISMA, which directs agency heads to provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access to, use, disclosure, disruption, modification, or destruction of information and information systems.

[47] On December 21, 2004, OMB revised the circular, which became effective in FY 2006, to strengthen requirements for conducting management's assessment of internal control over financial reporting and to emphasize the need for agencies to integrate and coordinate internal control assessments with other internal-control-related activities. The circular implements the Federal Managers' Financial Integrity Act (FMFIA). This Act is applicable to the FDIC because of provisions in the Chief Financial Officers Act of 1990 regarding annual reporting by government corporations on their internal accounting and administrative control systems. The FDIC has determined that as long as it develops internal controls that are consistent with the goals of FMFIA, the FDIC will have met its legal obligations under the circular.

[48] OMB A-130, Appendix III, establishes minimum controls for federal automated information security programs. The FDIC has determined that portions of the circular apply to the FDIC, while other portions do not apply. The FDIC has also determined that OMB A-130, Appendix III, requires the FDIC to implement and maintain an information security program consistent with government-wide policies, standards, and procedures issued by OMB and the Department of Commerce.

Government oversight agencies, such as GAO and OMB, and recognized standards-setting organizations such as NIST have identified fundamental management principles and controls needed to implement an effective information security program.[49] The controls were defined with the publication of FIPS PUB 200 and NIST SP 800-53 Rev. 1, and an assessment methodology was outlined in a draft assessment guide in SP 800-53A. SP 800-53 Rev. 1 defines a minimum set of security controls for the non-national security systems of all federal agencies. These security controls were selected based on the potential impact that could occur to the agency should there be a loss of confidentiality, integrity, or availability of the information or information system. The publication defines 17 management, operational, and technical security control families that are integral to securing any federal information system.

In addition to the SP 800-53 Rev. 1 controls for securing systems, SP 800-100 describes other controls for agency-wide management of a security program. Based on our analysis of SP 800-100 and the FDIC's business and IT environment, we identified two additional security program control families, *Information Security Governance/Performance Measures* and *Enterprise Architecture* for testing in 2007. Table 19 lists the security control classes and related security control families.

The FISMA evaluation framework consists of assessing the program control class on an agency-wide basis and assessing management, operational, and technical control classes on a sample of systems. The assessment of control families leverages the results of testing of a selection of the control objectives that make up the control family. We selected systems, control families, and individual controls for testing based on how important the system is to the FDIC, the control family is to the system, and the control is to the control family. We considered risk, costs, results of internal and external reviews, government-wide and FDIC initiatives and goals, the maturity of the security program, and other factors in selecting our samples. For FY 2007, the evaluated information systems included the Windows Servers and Personal Systems GSS. The Personal Systems GSS includes the FDIC's Windows XP desktop, and the Windows Servers GSS includes Windows NT/2000/2003 server operating systems.

Table 19: Security Control Classes and Families

Security Control Class	Security Control Family
Program	Information Security Governance/Performance Measures
	Enterprise Architecture
	Capital Planning*
Management	Risk Assessment
	Planning
	System and Services Acquisition*
	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
	Physical and Environmental Protection
	Contingency Planning
	Configuration Management
	Maintenance
	System and Information Integrity
	Media Protection
	Incident Response
	Awareness and Training
Technical	Identification and Authentication
	Access Control
	Audit and Accountability
	System and Communications Protection*

Source: KPMG analysis of NIST guidance.
*This control family was not included in the FY2007 FISMA evaluations of the FDIC's information security program.

[49] GAO Executive Guide, Information Security Management: *Learning From Leading Organizations*; and OMB A-130, Appendix III; NIST SP 800-14; SP 800-12; and SP 800-53.

Laws and Regulations

The references listed below represent the laws and regulations that were considered in the performance of our audit. Some of the references are statutes and regulatory sources, whose provisions may or may not be legally binding on the FDIC; see individual references for further information. Statutory and regulatory sources that are not binding on the FDIC can provide statements of prudent business practices. The Internet sites and the various references below are subject to change.

Federal Statutes

Federal Information Security Management Act (FISMA) of 2002 (title III, *E-Government Act of 2002)*, Pub. L. No. 107-347, dated December 17, 2002.
http://csrc.nist.gov/policies/FISMA-final.pdf

This Act requires federal agencies, including the FDIC, to develop, document, and implement an agency-wide information security program that provides security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA directs agencies to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluation to OMB.

Federal Managers' Financial Integrity Act of 1982, Pub. L. No. 97-255, dated September 8, 1982.
http://www.whitehouse.gov/omb/financial/fmfia1982.html

The FDIC has determined that portions of the FMFIA are applicable to the FDIC by reference in the Chief Financial Officers Act. In general, the goals of FMFIA are that agency obligations and costs comply with applicable law; assets are guarded against waste and loss; and revenue and expenditures are properly accounted for, so that reliable financial statements can be prepared.

Government Performance and Results Act of 1993, Pub. L. No. 103-62, dated August 3, 1993.
http://www.sc.doe.gov/bes/archives/plans/GPRA_PL103-62_03AUG93.pdf

The Act requires most federal agencies, including the FDIC, to develop a strategic plan that broadly defines the agency's mission and vision, an annual performance plan that translates the vision and goals of the strategic plan into measurable objectives, and an annual performance report that compares actual results against planned goals.

The Chief Financial Officers (CFO) Act of 1990, Pub. L. No. 101-576, dated November 15, 1990.
http://www.acq.osd.mil/me/pdfs/CFOA.pdf

This Act requires government corporations, such as the FDIC, to prepare annual management reports containing statements regarding the corporation's internal control systems, consistent with FMFIA.

The Privacy Act of 1974, Pub. L. 93-579, dated Dec. 31, 1974.
http://www.usdoj.gov/oip/privstat.htm

The Act, which is applicable to the FDIC, requires agencies to have appropriate administrative, technical, and physical safeguards over the security and confidentiality of agency records.

Regulation and Presidential Directive

5 Code of Federal Regulations Part 930, Subpart C, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems,* dated June 14, 2004.
http://csrc.nist.gov/policies/OPM-June2004-updated-sectrainaware.html

These regulations require agencies, including the FDIC, to develop plans for security awareness and training with respect to federal information systems, including role-specific training.

Homeland Security Presidential Directive–12*, Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004.
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

This presidential directive requires agencies to develop and implement a mandatory, government-wide standard for secure and reliable forms of identification. According to OMB guidance for implementing HSPD-12, government corporations are encouraged to comply with the directive. The FDIC is voluntarily complying with this directive.

OMB Circulars

OMB Circular No. A-123, *Management Responsibility for Internal Control*, dated December 21, 2004.
http://www.whitehouse.gov/omb/circulars/a123/a123_rev.pdf

This circular, which implements FMFIA, sets forth the requirements for agency evaluation of and reporting on internal controls as well as reporting on financial management systems. The FDIC has determined that this circular is applicable to the FDIC; specifically, as long as the FDIC's internal controls are consistent with the goals of the FMFIA, the FDIC will have met its obligations under this circular.

OMB Circular No. A-127, *Financial Management Systems*, dated July 23, 1993, as revised.
http://www.whitehouse.gov/omb/circulars/a127/a127.html

This circular prescribes policies for agencies to follow in developing, evaluating and reporting on their financial management systems. The FDIC has determined that to the extent that the Circular articulates FMFIA's standards, the FDIC should adhere to those standards.

OMB Circular No. A-130, *Management of Federal Information Resources,* Appendix III, *Security of Federal Automated Information Resources*, dated November 28, 2000.
http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf

This appendix establishes a minimum set of controls to be included in federal information security programs. Most of its provisions are applicable to the FDIC.

OMB Security-Related Memoranda

The following documents can be found at *http://www.whitehouse.gov/omb/memoranda*.

M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated September 26, 2003.

This memorandum implements section 208 of the E-Government Act, which applies to the FDIC. Accordingly, it addresses requirements for agency privacy impact analyses and website disclosures.

M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 5, 2005.

This memorandum provides implementing instructions for HSPD-12. According to the memorandum, government corporations are encouraged to comply with HSPD-12.

M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006.

This memorandum describes agency responsibility for safeguarding PII and requires reviews of related policies and procedures. The FDIC's intent is to comply with this memorandum or take it under consideration.

M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006.

This memorandum describes protection for agency remote or mobile systems and the need for logging certain data extracts. The FDIC's intent is to comply with this memorandum or take it under consideration.

M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006.

This memorandum requires agencies to report computer incidents to a central federal incident-reporting center. The FDIC's intent is to comply with this memorandum or take it under consideration.

M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, dated March 22, 2007.

Agencies that upgrade their Windows operating systems are to adopt certain interagency security configurations. The FDIC determined that while OMB has power to require that the FDIC develop policies and provide security protections, OMB cannot compel the FDIC to take specific actions of OMB's choosing.

M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

Agencies are required to develop a breach (unauthorized access) notification policy to implement other controls to protect PII. The FDIC is voluntarily complying with this memorandum.

M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 25, 2007.

The FDIC's practice is to comply with OMB's FISMA instructions.

Selected NIST Federal Information Processing Standards (FIPS)

NIST FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

This publication contains standards for security characterizations of federal information and information systems, as required by FISMA. The publication seeks to promote effective management and oversight of information security programs. Because the FDIC is not an executive agency for purposes of the publication, this publication is not legally applicable to the FDIC, but the FDIC follows its principles.

NIST FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006.
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

This publication specifies minimum security requirements for federal information systems in 17 security-related areas. The FDIC considers these requirements as reasonable best practices that the FDIC should seek to follow.

NIST FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, dated March 2006.
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

This publication implements HSPD-12. The FDIC is voluntarily complying with FIPS PUB 201.

Selected NIST Special Publications

In general, these NIST SPs are, by their own terms, guidelines (rather than mandatory requirements) for agencies in implementing their IT operations. The following documents may be found at: *http://csrc.nist.gov/publications/nistpubs/*.

SP 800-12, *An Introduction to Computer Security: The NIST Handbook*
SP 800-18, Rev. 1, *Guide for Developing Security Plans for Information Technology Systems*
SP 800-30, *Risk Management Guide for Information Technology Systems*
SP 800-34, *Contingency Planning Guide for Information Technology Systems*
SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
SP 800-40, Version 2, *Procedures for Handling Security Patches*
SP 800-46, Version 2 (Draft), *User's Guide to Securing External Devices for Telework and Remote Access*
SP 800-47, *Security Guide for Interconnecting Information Technology Systems*
SP 800-50, *Building an Information Technology Security Awareness and Training Program*
SP 800-53 Rev. 1, *Recommended Security Controls for Information Systems*
SP 800-53A (Draft June 2007), *Guide for Assessing the Security Controls in Federal Information Systems*
SP 800-55, *Security Metrics Guide for Information Technology Systems*
SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
SP 800-61, *Computer Security Incident Handling Guide*
SP 800-63, *Electronic Authentication Guideline*
SP 800-64, *Security Considerations in the Information System Development Life Cycle*

SP 800-65, ***Integrating Security into the Capital Planning and Investment Control Process***
SP 800-68, ***Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist***
SP 800-70, ***Security Configurations Checklists Program for IT Products: Guidance for Checklists Users and Developers***
SP 800-100, ***Information Security Handbook: A Guide for Managers***

APPENDIX II – STATUS OF OIG'S FY2006 FISMA KEY STEPS

Key Steps To Improve Information Security	Action Completed	Action in Progress
Certification and Accreditation: 1) Continue to place priority attention on certifying and accrediting the FDIC's non-major application systems that process sensitive data.	✓	
Audit and Accountability: 2) Develop a risk-based, enterprise-wide approach for (a) monitoring user access privileges in information systems and (b) generating and reviewing audit logs for the FDIC's inventory of information systems.		✓
OMB Privacy: 3) Ensure that all sensitive data stored on mobile FDIC computing devices is encrypted consistent with OMB's June 23, 2006 memorandum, *Protection of Sensitive Agency Information*.		✓
Information Security Governance: 4) Complete the FDIC's information security risk management program methodology by defining procedures for performing (a) continuous monitoring of system security controls after accreditation and (b) contingency planning for systems.	✓	
Enterprise Architecture: 5) Define more fully the FDIC's information security standards, and integrate these standards into the Corporation's EA.		✓
Enterprise Architecture: 6) Enhance the FDIC's inventory of information systems by: (a) identifying systems used or operated by contractors and other organizations on behalf of the FDIC; (b) including interfaces between each system in the inventory and all other systems and networks, including those not operated by, or under the control of, the FDIC; and (c) leveraging the EA to centrally manage, track, and report risk-management-related information, such as system categorization and test and authorization dates.	✓ (a) and (c)	✓ (b)
System and Information Integrity: 7) Strengthen oversight of contractors with access to sensitive information and systems by ensuring that (a) contractor IT equipment connected to the FDIC's network is routinely scanned for security vulnerabilities and the results are addressed in a timely manner, and (b) confidentiality agreements are executed in accordance with FDIC policy.	✓	
Configuration Management: 8) Strengthen change-control procedures related to mainframe system software to ensure that system software programs are formally documented and that changes are formally controlled and approved.	✓	
Capital Planning: 9) Improve the FDIC's information security cost-management practices in order to facilitate resource and investment decisions.	The FDIC did not agree with the OIG's key step.	

APPENDIX III – SUMMARY OF CONTROLS TESTED

The table below lists the security controls selected for testing from NIST SP 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*, dated December 2006. KPMG performed testing on a sample of controls identified in the "Controls Tested FY 2007" column. KPMG selected security controls for testing based on the risk and applicability to the FDIC's common controls, Windows Servers GSSs, and remote access environments. KPMG considered the control objective's rated requirement (low, moderate, or high), when selecting the security control for testing. In many instances, a security control either did not apply to the information systems selected for testing or was applicable only for information with a high FIPS 199 impact rating. None of information systems KPMG evaluated had a high FIPS 199 impact rating.

NIST SP 800-53 Rev. 1 Control			Controls Tested FY 2006	Controls Tested FY 2007
Family	**No.**	**Name**		
Management Control Class				
Risk Assessment (RA)	RA-1	Risk Assessment Policy and Procedures	✓	✓
	RA-2	Security Categorization	✓	✓
	RA-3	Risk Assessment	✓	✓
	RA-4	Risk Assessment Update	✓	✓
	RA-5	Vulnerability Scanning	✓	✓
Planning (PL)	PL-1	Security Planning Policy and Procedures	✓	✓
	PL-2	System Security Plan		✓
	PL-3	System Security Plan Update		✓
	PL-4	Rules of Behavior	✓	
	PL-5	Privacy Impact Assessment	✓	✓
	PL-6	Security-Related Activity Planning		
System and Services Acquisition (SA)	SA-1	System and Services Acquisition Policy and Procedures	✓	✓
	SA-2	Allocation of Resources		
	SA-3	Life Cycle Support		✓
	SA-4	Acquisitions		✓
	SA-5	Information System Documentation		✓
	SA-6	Software Usage Restrictions	✓	✓
	SA-7	User Installed Software	✓	
	SA-8	Security Engineering Principles		
	SA-9	External Information System Services		
	SA-10	Developer Configuration Management		
	SA-11	Developer Security Testing		
Certification, Accreditation, and	CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	✓	✓

NIST SP 800-53 Rev. 1 Control			Controls Tested FY 2006	Controls Tested FY 2007
Family	**No.**	**Name**		
Security Assessments (CA)	CA-2	Security Assessments	✓	
	CA-3	Information System Connections	✓	
	CA-4	Security Certification	✓	✓
	CA-5	Plan of Action and Milestones	✓	✓
	CA-6	Security Accreditation	✓	✓
	CA-7	Continuous Monitoring		✓
Operational Control Class				
Physical and Environmental Protection (PE)	PE-1	Physical and Environmental Protection Policy and Procedures	✓	✓
	PE-2	Physical Access Authorizations	✓	✓
	PE-3	Physical Access Control	✓	✓
	PE-4	Access Control for Transmission Medium		
	PE-5	Access Control for Display Medium		
	PE-6	Monitoring Physical Access	✓	✓
	PE-7	Visitor Control	✓	✓
	PE-8	Access Records	✓	✓
	PE-9	Power Equipment and Power Cabling	✓	
	PE-10	Emergency Shutoff	✓	
	PE-11	Emergency Power	✓	
	PE-12	Emergency Lighting	✓	
	PE-13	Fire Protection	✓	
	PE-14	Temperature and Humidity Controls	✓	
	PE-15	Water Damage Protection	✓	
	PE-16	Delivery and Removal		
	PE-17	Alternate Work Site	✓	
	PE-18	Location of Information System Components		
	PE-19	Information Leakage		
Personnel Security (PS)	PS-1	Personnel Security Policy and Procedures	✓	✓
	PS-2	Position Categorization	✓	✓
	PS-3	Personnel Screening	✓	✓
	PS-4	Personnel Termination	✓	✓
	PS-5	Personnel Transfer	✓	✓
	PS-6	Access Agreements	✓	✓
	PS-7	Third-Party Personnel Security	✓	✓
	PS-8	Personnel Sanctions		

NIST SP 800-53 Rev. 1 Control			Controls Tested FY 2006	Controls Tested FY 2007
Family	**No.**	**Name**		
Contingency Planning (CP)	CP-1	Contingency Planning Policy and Procedures	✓	✓
	CP-2	Contingency Plan	✓	✓
	CP-3	Contingency Training	✓	✓
	CP-4	Contingency Plan Testing and Exercises	✓	✓
	CP-5	Contingency Plan Update	✓	✓
	CP-6	Alternate Storage Sites	✓	✓
	CP-7	Alternate Processing Sites	✓	✓
	CP-8	Telecommunications Services	✓	✓
	CP-9	Information System Backup	✓	✓
	CP-10	Information System Recovery and Reconstitution		✓
Configuration Management (CM)	CM-1	Configuration Management Policy and Procedures	✓	✓
	CM-2	Baseline Configuration	✓	✓
	CM-3	Configuration Change Control	✓	✓
	CM-4	Monitoring Configuration Changes	✓	
	CM-5	Access Restrictions for Change	✓	✓
	CM-6	Configuration Settings	✓	✓
	CM-7	Least Functionality	✓	✓
	CM-8	Information System Component Inventory		✓
Maintenance (MA)	MA-1	System Maintenance Policy and Procedures	✓	✓
	MA-2	Controlled Maintenance	✓	✓
	MA-3	Maintenance Tools		
	MA-4	Remote Maintenance		
	MA-5	Maintenance Personnel		
	MA-6	Timely Maintenance		
System and Information Integrity (SI)	SI-1	System and Information Integrity Policy and Procedures	✓	✓
	SI-2	Flaw Remediation	✓	✓
	SI-3	Malicious Code Protection	✓	✓
	SI-4	Information System Monitoring Tools and Techniques	✓	✓
	SI-5	Security Alerts and Advisories	✓	
	SI-6	Security Functionality Verification		
	SI-7	Software and Information Integrity		
	SI-8	Spam Protection	✓	

NIST SP 800-53 Rev. 1 Control			Controls Tested FY 2006	Controls Tested FY 2007
Family	**No.**	**Name**		
	SI-9	Information Input Restrictions		
	SI-10	Information Accuracy, Completeness, Validity, and Authenticity		
	SI-11	Error Handling		
	SI-12	Information Output Handling and Retention		
Media Protection (MP)	MP-1	Media Protection Policy and Procedures	✓	✓
	MP-2	Media Access	✓	
	MP-3	Media Labeling		✓
	MP-4	Media Storage	✓	✓
	MP-5	Media Transport	✓	
	MP-6	Media Sanitization and Disposal	✓	
Incident Response (IR)	IR-1	Incident Response Policy and Procedures	✓	✓
	IR-2	Incident Response Training	✓	
	IR-3	Incident Response Testing and Exercises		
	IR-4	Incident Handling	✓	✓
	IR-5	Incident Monitoring	✓	
	IR-6	Incident Reporting	✓	✓
	IR-7	Incident Response Assistance	✓	
Awareness and Training (AT)	AT-1	Security Awareness and Training Policy and Procedures	✓	✓
	AT-2	Security Awareness	✓	✓
	AT-3	Security Training	✓	✓
	AT-4	Security Training Records		✓
	AT-5	Contacts with Security Groups and Associations		
Technical Control Class				
Identification and Authentication (IA)	IA-1	Identification and Authentication Policy and Procedures	✓	✓
	IA-2	User Identification and Authentication	✓	✓
	IA-3	Device Identification and Authentication		
	IA-4	Identifier Management	✓	✓
	IA-5	Authenticator Management	✓	
	IA-6	Authenticator Feedback	✓	✓
	IA-7	Cryptographic Module Authentication		
Access Control (AC)	AC-1	Access Control Policy and Procedures	✓	✓
	AC-2	Account Management	✓	✓

NIST SP 800-53 Rev. 1 Control			Controls Tested FY 2006	Controls Tested FY 2007
Family	**No.**	**Name**		
	AC-3	Access Enforcement	✓	✓
	AC-4	Information Flow Enforcement		
	AC-5	Separation of Duties		✓
	AC-6	Least Privilege	✓	✓
	AC-7	Unsuccessful Login Attempts	✓	✓
	AC-8	System Use Notification	✓	✓
	AC-9	Previous Logon Notification		
	AC-10	Concurrent Session Control		
	AC-11	Session Lock	✓	
	AC-12	Session Termination	✓	✓
	AC-13	Supervision and Review – Access Control		✓
	AC-14	Permitted Actions without Identification or Authentication	✓	
	AC-15	Automated Marking		
	AC-16	Automated Labeling		
	AC-17	Remote Access	✓	✓
	AC-18	Wireless Access Restrictions		
	AC-19	Access Control for Portable and Mobile Systems		✓
	AC-20	Use of External Information System		✓
Audit and Accountability (AU)	AU-1	Audit and Accountability Policy and Procedures	✓	✓
	AU-2	Auditable Events	✓	✓
	AU-3	Content of Audit Records	✓	✓
	AU-4	Audit Storage Capacity	✓	✓
	AU-5	Response to Audit Processing Failures	✓	✓
	AU-6	Audit Monitoring, Analysis, and Reporting	✓	✓
	AU-7	Audit Reduction and Report Generation		
	AU-8	Time Stamps	✓	✓
	AU-9	Protection of Audit Information	✓	✓
	AU-10	Non-repudiation		✓
	AU-11	Audit Record Retention	✓	
System and Communications Protection (SC)	SC-1	System and Communications Protection Policy and Procedures	✓	✓
	SC-2	Application Partitioning		✓
	SC-3	Security Function Isolation		

NIST SP 800-53 Rev. 1 Control			Controls Tested FY 2006	Controls Tested FY 2007
Family	**No.**	**Name**		
	SC-4	Information Remnants		
	SC-5	Denial of Service Protection		
	SC-6	Resource Priority		
	SC-7	Boundary Protection		✓
	SC-8	Transmission Integrity		
	SC-9	Transmission Confidentiality	✓	✓
	SC-10	Network Disconnect		
	SC-11	Trusted Path		
	SC-12	Cryptographic Key Establishment and Management		
	SC-13	Use of Cryptography		
	SC-14	Public Access Protections		
	SC-15	Collaborative Computing		
	SC-16	Transmission of Security Parameters		
	SC-17	Public Key Infrastructure Certificates		
	SC-18	Mobile Code		✓
	SC-19	Voice Over Internet Protocol		
	SC-20	Secure Name/Address Resolution Service (Authoritative Source)		
	SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)		
	SC-22	Architecture and Provisioning for Name/Address Resolution Service		
	SC-23	Session Authenticity		

APPENDIX IV – OMB SECURITY QUESTIONS

Section C- Inspector General: Questions 1 and 2

Agency Name: **Federal Deposit Insurance Corporation (FDIC)** **Submission Date:** **9/26/07**

Question 1: FISMA System Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Question 2: Certification and Accreditation, Security Control Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						**Question 2**					
		a. Agency Systems		**b. Contractor Systems**		**c. Total Number of Systems** (Agency and Contractor systems)		**a. Number of systems certified and accredited**		**b. Number of systems for which security controls have been tested and reviewed in the past year**		**c. Number of systems for which contingency plans have been tested in accordance with policy**	
Bureau Name	**FIPS 199 Risk Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
FDIC	High	0	0	0	0	0	0	0	N/A	0	N/A	0	N/A
	Moderate	16	2	0	0	16	2	2	100%	2	100%	2	100%
	Low	0	0	0	0	0	0	0	N/A	0	N/A	0	N/A
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Total	**16**	**2**	**0**	**0**	**16**	**2**	**2**	**100%**	**2**	**100%**	**2**	**100%**

Section C- Inspector General: Questions 3		
Agency Name: Federal Deposit Insurance Corporation (FDIC)		**Submission Date:** 9/26/07
Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory		
3.a.	**The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.** Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Frequently, for example, approximately 71-80% of the time
3.b.	**The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.** Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	- The inventory is approximately 71-80% complete
	Comments: Based on KPMG's review of the system inventory, the number of system interfaces could not be verified because the system inventory does not identify system interfaces between each system and all other systems or networks, including those not operated by, or under, the control of the agency. The FDIC does include this information on an Application Security Assessment (ASA). However, KPMG noted that ASAs containing this interfacing information have not been completed for all applications.	
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually. Yes or No.**	Yes

3.f. **If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI)	Agency or Contractor system?
Division of Administration (DOA)	PEGASYS	Not Applicable	Agency

Number of known systems missing from inventory:	1

Section C- Inspector General: Question 4		
Agency Name: Federal Deposit Insurance Corporation (FDIC)		**Submission Date: 9/26/07**
Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process		
Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided. **For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.** **Response Categories:** **- Rarely- for example, approximately 0-50% of the time** **- Sometimes- for example, approximately 51-70% of the time** **- Frequently- for example, approximately 71-80% of the time** **- Mostly- for example, approximately 81-95% of the time** **- Almost Always- for example, approximately 96-100% of the time**		
4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Frequently- for example, approximately 71-80% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	**-** Mostly- for example, approximately 81-95% of the time
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	- Almost Always, for example, approximately 96-100% of the time
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	IG findings are incorporated into the POA&M process.	- Frequently- for example, approximately 71-80% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	- Almost Always, for example, approximately 96-100% of the time
POA&M process comments: Although the FDIC has developed policy and guidelines for preparing and managing system-level POA&Ms, the FDIC needed to modify its POA&M procedures to ensure that system-level POA&Ms either reflect consolidation of, or are accompanied by, other FDIC plans to correct all relevant IT security weaknesses, including weaknesses identified in GAO and FDIC OIG reports and any other IT security review. C&A guidelines provide that ST&E weaknesses are included in system-level POA&Ms. In addition, the FDIC tracks system-level security weaknesses in a number of standalone spreadsheets and databases based on how the weakness is identified. For example, system-level security weaknesses identified by the GAO, OIG, or internal FDIC reviews are managed in the FDIC's IRIS; where as system-level security weaknesses identified by ST&Es are managed in system-level POA&Ms. DIT can better integrate its management of security weaknesses by developing system-level POA&Ms that include all relevant security weaknesses, either through consolidation of other documents used to identify and track weaknesses or as a POA&M attachment. At the close of KPMG's fieldwork, DIT began including all IT security weaknesses on system-level POA&Ms.		

Section C- Inspector General: Questions 5

Agency Name: Federal Deposit Insurance Corporation (FDIC) **Submission Date: 9/26/07**

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	The IG rates the overall quality of the Agency's certification and accreditation process as: Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory

5.b.	The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other:	

C&A process comments: The FDIC established a C&A program consisting of policies, procedures, and guidelines; key personnel, such as a Certification Agent and Authorizing Official; an independent ST&E process; and POA&Ms for tracking and remediating security weaknesses. The FDIC has fully certified and accredited all of its major information systems, including GSSs and major applications, consistent with NIST security standards and guidelines. In addition, the FDIC revised its information security risk management methodology in June 2006 to achieve cost efficiencies in its C&A processes by consolidating its minor information systems that process sensitive data through an aggregation process. While these accomplishments are significant, KPMG and OIG testing of security controls during FY 2007 noted control weaknesses in GSSs, that recently completed the C&A process. More-thorough testing during the ST&E phase or through enhanced Continuous Monitoring activities of these GSSs likely would have identified these control deficiencies. Thus, KPMG has rated the FDIC's C&A processes as "Satisfactory."

Section C- Inspector General: Questions 6 and 7		
Agency Name: Federal Deposit Insurance Corporation (FDIC)		**Submission Date: 9/26/07**
Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6.a.	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory
	Comments: The FDIC OIG has prepared a report AUD-07-013, entitled, *Response to Privacy Program Information Request in OMB's Fiscal Year 2007 Reporting Instructions for FISMA and Agency Privacy Management*, scheduled for issuance on September 26, 2007. Please refer to this public report for additional information regarding the FDIC's privacy program.	
6.b.	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory
	Comments: The FDIC OIG has prepared a separate report AUD-07-013, titled *Response to Privacy Program Information Request in OMB's Fiscal Year 2007 Reporting Instructions for FISMA and Agency Privacy Management*, scheduled for issuance on September 26, 2007. Please refer to this public report for additional information regarding the FDIC's Privacy Program.	
Question 7: Configuration Management		
7.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
	Comments: None.	
7.b.	**Approximate the extent to which applicable information systems apply common security configurations established by NIST.** **Response categories:** - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	- Mostly, for example, approximately 81-95% of the time
	Comments: As part of the 2007 FISMA Evaluation at the FDIC, KPMG reviewed the FDIC's Personal Systems GSS, which included Windows XP. KPMG compared the FDIC's Windows XP security configuration settings to those established by NIST SP 800-68 and noted that 27 of the 133 identified settings were not in compliance. KPMG noted that the FDIC historically follows industry best practices established by NIST or the National Security Agency and then tailors the settings for compatibility with its environment. Based on this observation and the fact that this is the first year that configuration settings are being directly compared to those established by NIST, our response is ***Mostly, for example, approximately 81-95% of the time.***	

Section C- Inspector General: Questions 8, 9, 10 and 11		
Agency Name: Federal Deposit Insurance Corporation (FDIC)		**Submission Date: 9/26/07**
Question 8: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
8.a.	**The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**	Yes
8.b.	**The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)**	Yes
8.c.	**The agency follows defined procedures for reporting to law enforcement Yes or No.**	Yes
	Comments: As part of the 2007 FISMA Evaluation, KPMG selected a non-statistical sample of 20 incidents and verified that CSIRT followed their documented policies and procedures when handling the incidents.	
Question 9: Security Awareness Training		
9	**Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?** **Response Choices include:** **- Rarely, or, approximately 0-50% of employees have sufficient training** **- Sometimes, or approximately 51-70% of employees have sufficient training** **- Frequently, or approximately 71-80% of employees have sufficient training** **- Mostly, or approximately 81-95% of employees have sufficient training** **- Almost Always, or approximately 96-100% of employees have sufficient training**	- Almost Always, or approximately 96-100% of employees have sufficient training
Question 10: Peer-to-Peer File Sharing		
10	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.	Yes
Question 11: E-Authentication Risk Assessment		
11	The agency has completed system e-authentication risk assessments. Yes or No.	Yes

APPENDIX V – GLOSSARY OF TERMS

Term	Definition
Access Control	The ability to ensure that only authorized users can access system resources in authorized ways.
Adequate Security	Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, information.
Audit Trail	A series of records of computer-related events about an operating system, an application, or user activities. An information system may have several audit trails, each devoted to a particular type of activity. The terms audit trail and audit log are used synonymously in this report.
Auditable Event	An event is any action that happens on a computer system. Examples include logging into a system, executing a program, and opening a file.
Biometrics	One of various technologies that utilize behavioral or physiological characteristics to determine or verify identity. For example, a fingerprint scan is a commonly used biometric.
Encryption	In cryptography, it is the mean and method for rendering information unintelligible.
Firmware	A computer program that is embedded in a hardware device. It can also be provided on flash read-only memory or as a binary image file that can be uploaded onto existing hardware by a user.
General Support System (GSS)	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Hotfixes	A single, cumulative package that includes one or more files that are used to address a problem in a product. Hotfixes address a specific customer situation and may not be distributed outside the customer organization.
Intrusion Detection System (IDS)	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.
Least Privilege	Refers to the practice of restricting a user's access to only those resources needed to perform official duties.
Log	A record of the events occurring within an organization's systems and networks. Logs are composed of entries that contain information related to a specific event that occurred within a system or network.
Major Applications	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of, the information in the application.
National Institute of Standards and Technology (NIST)	A non-regulatory federal agency within the Department of Commerce's Technology Administration. As part of its responsibilities, NIST develops and publishes technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive, but unclassified, information in federal computer systems.
Rational Unified Process (RUP®)	An iterative software development process created by the Rational Software Corporation, now a division of IBM. The RUP is not a single concrete prescriptive process, but rather an adaptable process framework that the FDIC has customized for its systems development life cycle.
Source Code	A set of programming language instructions that must be translated into machine instructions before the program can run.
Security Test & Evaluation (ST&E)	An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system