Office of Inspector General

September 2006
Report No. 06-019

Responses to Security-Related Questions in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management

Office of Audits

oig

Office of Audits

Responses to Security-Related Questions in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management

Background and Purpose of Audit

To achieve its mission, the FDIC relies heavily on automated information systems to collect, process, and store vast amounts of banking information. Ensuring the integrity, availability, and appropriate confidentiality of this information requires a strong, enterprise-wide information security program.

The Federal Information Security Management Act of 2002 (FISMA) directs federal agencies 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), the Comptroller General, and various congressional committees. In addition, the OMB instructs agencies and cognizant Inspectors General (IG) to answer specific questions related to the status of their security program as part of the FISMA evaluation.

The objective of this audit was to answer specific security-related questions addressed to agency IGs in the OMB's July 17, 2006 memorandum entitled, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. We contracted with KPMG LLP (KPMG) to perform this audit.

To view the full report, go to www.fdicig.gov/2006reports.asp

Results of Audit

As KPMG's responses to the OMB questions indicate, the FDIC has implemented plans of action and milestones, an incident response capability, and security awareness and training that substantially address the criteria used by the OMB for assessing the status of those aspects of agency security programs. However, continued management attention is needed in some security control areas—such as information systems inventory, oversight of contractor systems, certification and accreditation, and security configuration management—to ensure compliance with FISMA and consistency with National Institute of Standards and Technology standards and guidelines. KPMG's work did not identify any significant deficiencies in the FDIC's information security program warranting consideration as a potential material weakness as defined by the OMB.

The OMB questions focus on certain key components of the FDIC's information security program. We plan to issue a report entitled, *Independent Evaluation of the FDIC's Information Security Program-2006* (FDIC-OIG Report No. 06-022), that provides an overall assessment of the FDIC's information security program, including detailed results of work performed in the areas covered by the OMB questions. The report also identifies key steps that the Corporation can take to strengthen its information security program.

Recommendations and Management Response

The focus of this audit was on responding to OMB's questions to the IGs. Accordingly, this report does not contain any recommendations. A written response was not required from the Corporation. However, the Corporation provided informal comments, which were considered and incorporated, as appropriate, into the report.

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

Office of Audits
Office of Inspector General

DATE: September 22, 2006

MEMORANDUM TO: Michael E. Bartell, Chief Information Officer and Director, Division of Information Technology

FROM: Russell A. Rau [Electronically produced version; original signed by Russell A. Rau]
Assistant Inspector General for Audits

SUBJECT: KPMG LLP Report Entitled, *Responses to Security-Related Questions in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management* (Report No. 06-019)

Attached is a copy of the subject report prepared by KPMG LLP (KPMG) under a contract with the FDIC Office of the Inspector General. Please refer to the Executive Summary for the overall results of the audit. KPMG did not make any recommendations in this report. Accordingly, no additional actions are required by the FDIC.

If you have questions concerning the report, please contact Stephen M. Beard, Deputy Assistant Inspector General for Audits, at (703) 562-6352, or Mark Mulholland, Director, Systems Management and Security Audits, at (703) 562-6316. We appreciate the courtesies extended to the staff during the audit.

Attachment

cc: James H. Angel, Jr., Director, OERM
Rack D. Campbell, DIT

Responses to Security-Related Questions in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management
(Report Number 06-019)

Prepared for the
Federal Deposit Insurance Corporation
Office of Inspector General

FINAL REPORT

Prepared by:
KPMG LLP
Advisory Services, Federal Practice
2001 M Street, NW
Washington, DC 20036
202-533-3000

TABLE OF CONTENTS

ACRONYMS

C&A	Certification and Accreditation
CIO	Chief Information Officer
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
FY	Fiscal Year
IG	Inspector General
IT	Information Technology
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
ST&E	Security Test and Evaluation

INTRODUCTION

On July 17, 2006, the Office of Management and Budget (OMB) issued a memorandum entitled, *FY [Fiscal Year] 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The OMB memorandum directs agency Chief Information Officers (CIO) and Inspectors General (IG) to answer a series of questions related to the performance of their respective agency's information security program. The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct a performance audit for which the objective was to prepare responses to the OMB questions directed to the IGs.

The responses to the OMB questions are based on the results of work KPMG performed in support of the FDIC OIG's 2006 independent security evaluation[1] required by the Federal Information Security Management Act (FISMA) of 2002. The work included assessing the information security policies, procedures, and practices for a representative subset of the FDIC's information systems[2] as required by FISMA. Such work also included an assessment of common security controls applicable to one or more FDIC information systems and consideration of relevant information-security-related audits. In addition, the FDIC OIG has contracted with KPMG for a separate report containing information related to the FDIC's privacy program.[3] The information is also requested in OMB's reporting instructions.

Appendix I describes our objective, scope, and methodology. Appendix II contains the responses to each of the information-security-related questions in the format prescribed by the OMB Director.

BACKGROUND

Title III of the E-Government Act of 2002, commonly referred to as 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 systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA directs federal agencies to report annually to OMB, the Comptroller General, and various congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices, including compliance with FISMA. In addition, OMB instructs each agency

---

[1] *Independent Evaluation of the FDIC's Information Security Program-2006* (FDIC-OIG Report No. 06-022), scheduled for issuance in September, 2006.

[2] We performed a detailed analysis of the FDIC's local area network/wide area network and mainframe general support systems. We also performed a limited analysis of a contractor system (Central Data Repository).

[3] *Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management* (FDIC-OIG Report No. 06-018), dated September 22, 2006.

and its IG to answer specific questions as part of the agency's overall FISMA evaluation. OMB uses the agency FISMA reports for various purposes, such as helping to evaluate government-wide security performance, developing OMB's annual security report to the Congress, and assisting in improving and maintaining adequate agency security performance.

RESULTS OF AUDIT

As KPMG's responses to the OMB questions (see Appendix II) indicate, the FDIC has implemented plans of action and milestones, an incident response capability, and security awareness and training that substantially address the criteria used by the OMB for assessing the status of those aspects of agency security programs. However, continued management attention is needed in some security control areas—such as information systems inventory, oversight of contractor systems, certification and accreditation, and security configuration management—to promote compliance with FISMA and consistency with National Institute of Standards and Technology (NIST) standards and guidelines. KPMG's work did not identify any significant deficiencies in the FDIC's information security program warranting consideration as a potential material weakness as defined by the OMB.[4]

The OMB questions focus on certain key components of the FDIC's information security program. The OIG's report, *Independent Evaluation of the FDIC's Information Security Program-2006*, provides an overall assessment of the FDIC's information security program, including detailed results of audit work in the areas covered by the OMB questions. That report also identifies key steps that the Corporation can take to strengthen its information security program. KPMG was also under contract with the OIG to support this overall evaluation.

CORPORATION COMMENTS

A written response was not required for the report. However, the Corporation provided informal comments, which were considered and incorporated, as appropriate, into the report.

[4] The OMB defines a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified, and immediate or near-immediate corrective action must be taken. The OMB defines a material weakness as a deficiency that the agency head determines to be significant enough to be reported outside the agency (i.e., included in the annual management control report to the President and the Congress).

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the performance audit was to answer specific questions in OMB's July 17, 2006 memorandum (M-06-20) entitled, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. To accomplish this objective, KPMG relied primarily on the results of the work it performed in support of the OIG's independent FISMA security evaluation.[5] KPMG also performed certain other audit procedures that we deemed necessary to accomplish the audit objective. KPMG discussed each response to the OMB questions with the FDIC's Division of Information Technology's Information Security Staff.

KPMG did not separately perform procedures to review program performance measures, assess FDIC compliance with laws and regulations, evaluate the FDIC's management controls, or determine that computer-based data were valid and reliable. Such procedures were performed in support of the OIG's independent security evaluation required by FISMA. Additionally, while KPMG did not design tests to detect fraud, waste, abuse, and mismanagement, throughout the audit, KPMG and the OIG were sensitive to the potential for fraud, waste, abuse, and mismanagement.

KPMG performed the audit at the FDIC's Headquarters offices in Washington, D.C., and its Virginia Square facility in Arlington, Virginia. Also, KPMG visited the FDIC's disaster recovery site in Richmond, Virginia. KPMG conducted the performance audit from April through August 2006 in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States.

[5] *Independent Evaluation of the FDIC's Information Security Program-2006* (Report No. 06-022), scheduled for issuance on September 28, 2006.

RESPONSES TO OMB QUESTIONS

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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.

2. For each part of this question, identify actual performance in FY 06 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Agency Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	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	136	2	2	1	138	3	3	100.0%	2[a]	66.7%	2	66.7%
	Low	19	0	0	0	19	0	0	N/A	0	N/A	0	N/A
	Not Categorized	2	1	7	0	9	1	0	0.0%	0	0.0%	0	0.0%
	Total	**157**	**3**	**9[b]**	**1**	**166**	**4**	**3**	**75.0%**	**2**	**50.0%**	**2**	**50.0%**

[a] Security controls for one of the three certified and accredited systems had not been tested and evaluated during the current reporting period (i.e., August 1, 2005 through July 31, 2006). However, security control testing and evaluation was ongoing for this system at the time of the audit.

[b] KPMG was unable to independently verify the total number of contractor-maintained information systems because the FDIC's systems inventory did not fully incorporate these systems. KPMG's response to Question 1 reflects those contractor-maintained information systems that KPMG identified during the audit, as well as any systems identified for KPMG by the FDIC.

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and 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. Self-reporting of NIST Special Publication 800-26 and/or NIST 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. 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	- Sometimes, for example, approximately 51-70% of the time
3.b.1.	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: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 51-70% complete
3.b.2.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems: Pegasys We were unable to verify the number of system interfaces 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 FDIC. After the audit, the FDIC's Information Security Section provided an inventory of 12 major information systems with interfaces. We did not have the opportunity to determine whether the inventory was comprehensive; based on, and consistent with, FDIC policy and procedures; conforms to NIST guidance; or agrees with the FDIC's Enterprise Architecture. Missing Contractor Systems: None
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **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
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	Yes

Question 4		
Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. For items 4a.-4.f, the response categories are as follows: - 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.	- Mostly, for example, approximately 81-95% 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, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	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.	OIG findings are incorporated into the POA&M process.	- Mostly, for example, approximately 81-95% 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
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 information technology (IT) security weaknesses, including weaknesses identified in Government Accountability Office (GAO) and OIG reports and any other IT security review. Current certification and accreditation (C&A) guidelines provide that security test and evaluation (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 Internal Risks Information System; and system-level security weaknesses identified by system tests and evaluations are managed in system-level POA&Ms. The Division of Information Technology can better integrate its management of security weaknesses by developing system-level POA&Ms that include all relevant security weaknesses, either through consolidation or as a POA&M attachment.		

Question 5		
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. 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 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.		
	Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory
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. In February 2006, the OIG issued an audit report recognizing that the FDIC's C&A policies, procedures, and practices were satisfactory and consistent with federal security standards and guidelines but that opportunities for enhancements in some areas could be made (Report No. 06-007, *Audit of the FDIC's Security Certification and Accreditation Program*, dated February 2006). At the close of KPMG's audit, the FDIC was working to define information security risk management procedures for performing (a) continuous monitoring of its information systems after accreditation and (b) contingency planning of its information systems. The FDIC has fully certified and accredited all but one of its major applications and general support systems consistent with NIST security standards and guidelines. (The remaining major application is operating under an interim authority to operate.) 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 non-major information systems that process sensitive data through an aggregation process. However, more work remains to complete C&As for the FDIC's non-major information systems that process sensitive data.		

Question 6			
6.a.	Is there an agency wide security configuration policy? Yes or No.		Yes
	Comments: None		
6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency-wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.		
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows 2000 Professional	N/A	No	
Windows 2000 Server	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows 2003 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Solaris	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
HP-UX	N/A	No	
Linux	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Other.	N/A	No	
Comments: The results in the far right-hand column are derived from KPMG's analysis of the results from the FDIC's July 2006 Foundstone vulnerability scan and the June 2006 Cisco Router Auditing Tool data. Specifically, KPMG determined the extent to which the products KPMG sampled were consistent with the FDIC's configuration requirements and best practices.			

Question 7		
Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.		
7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes
Comments: None		
Question 8		
8	Has the agency ensured security training and awareness 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 9		
9	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