Office of Inspector General

September 2007
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

AUDIT REPORT

Office of Audits

oig

Office of Audits

Background and Purpose of Audit

In fulfilling its legislative mandate of insuring deposits, supervising financial institutions, and managing receiverships and in its role as a federal employer and acquirer of services, the FDIC creates and acquires a significant amount of personally identifiable information (PII) (e.g., name, Social Security number, or biometric records) related to depositors and borrowers at FDIC-insured financial institutions and FDIC employees and contractors. Much of the PII managed by the FDIC and its contractors falls within the scope of several statutes and regulations intended to protect such information from unauthorized disclosure.

On July 25, 2007, the Office of Management and Budget (OMB) issued Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The memorandum directs agency Inspectors General to provide relevant status information on agency privacy programs. In addition, the memorandum directs agency IGs to assess (1) the quality of their agencies' process for conducting privacy impact assessments (PIA) of systems containing PII and (2) the progress the agency is making in implementing PII safeguards recommended in OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 2, 2006. OMB defines a PIA as a process for (1) examining the risks of using information technology to collect, maintain, and disseminate PII from or about members of the public and for (2) identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

Consistent with the provisions of OMB Memorandum M-07-19, the objective of the audit was to assess the status of the FDIC's privacy program activities and initiatives. Our work focused on the status of the FDIC's efforts to address selected key provisions of privacy-related memoranda recently issued by OMB.

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

Report No. AUD-07-013
September 2007

Response to Privacy Program Information Request in OMB's Fiscal Year 2007 Reporting Instructions for FISMA and Agency Privacy Management

Results of Audit

The FDIC continues to take action to safeguard its PII and related systems and address privacy-related provisions of recent OMB memoranda. Of particular note, the FDIC has appointed a senior agency official for privacy, conducted privacy reviews prescribed by OMB, and provided employees and contractors with privacy-awareness training. Importantly, the FDIC has established a process for conducting PIAs of its information systems containing PII that is consistent with relevant privacy-related policy, guidance, and standards. In addition, the FDIC is making satisfactory progress in implementing the provisions of OMB Memorandum M-06-15. Further, the FDIC is working to complete a number of ongoing privacy program initiatives to safeguard its PII and related systems consistent with privacy-related statutes, policies, and guidelines. Such initiatives include:

- Deploying new software that automatically encrypts sensitive information stored on portable computing devices (e.g., laptops and flash drives).
- Conducting a comprehensive review of access controls over sensitive information stored on network shared drives throughout the Corporation.
- Ensuring that access to applications containing PII is appropriately limited.
- Referencing in corporate policy the FDIC's new breach notification plan and procedures for responding to PII breaches.
- Implementing measures to ensure technologies used to collect, use, store, and disclose PII allow for continuous auditing of compliance with stated privacy policies and practices.
- Logging all computer-readable data extracts from databases holding sensitive information and verifying that each extract, including sensitive data, has been erased within 90 days or its use is still required.

This report contains no recommendations. We plan to follow up on the status of these initiatives as part of future privacy reviews.

TABLE OF CONTENTS

ACRONYMS

CD/DVD	Compact Disk/Digital Versatile Disk
CIO	Chief Information Officer
CPO	Chief Privacy Officer
DIT	Division of Information Technology
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers' Financial Integrity Act
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
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Assessment
RUP®	Rational Unified Process
SP	Special Publication
SSN	Social Security Number
USB	Universal Serial Bus

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

Office of Audits
Office of Inspector General

DATE: September 26, 2007

MEMORANDUM TO: Michael E. Bartell, Chief Privacy Officer

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

SUBJECT: *Response to Privacy Program Information Request in OMB's Fiscal Year 2007 Reporting Instructions for FISMA and Agency Privacy Management*
(Report No. 07-013)

This report presents the results of our audit of the status of the FDIC's privacy program. We performed the audit in response to a request for privacy program information in the Office of Management and Budget's (OMB) July 25, 2007 Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act* [FISMA] *and Agency Privacy Management*. The OMB memorandum directs agency Inspectors General (IG) to provide relevant status information on agency privacy programs. In addition, the memorandum directs agency IGs to assess (1) the quality of their agencies' process for conducting privacy impact assessments (PIA)[1] of systems containing PII[2] and (2) the progress the agency is making in implementing PII safeguards recommended in OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006. As part of our audit, we assessed the status of the FDIC's efforts to address selected key provisions of privacy-related memoranda recently issued by OMB.

The objective of the audit was to assess the status of the FDIC's privacy program activities and initiatives. As part of our work, we followed up on privacy-related issues identified in prior audit reports, particularly, *The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005* (Report No. 07-003) issued in January 2007 and prepared by KPMG, LLP (KPMG) under contract with the FDIC Office of Inspector General (OIG). The OIG contracted separately with KPMG to evaluate and report on the

[1] According to OMB Memorandum M-07-19, a PIA is a process for (1) examining the risks and ramifications of using information technology (IT) to collect, maintain, and disseminate personally identifiable information (PII) from or about members of the public and for (2) identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

[2] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, defines PII as information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

FDIC's information security program and practices pursuant to FISMA. As part of its information security program evaluation, KPMG prepared responses to security-related questions directed to agency IGs in OMB Memorandum M-07-19. KPMG's security program evaluation report,[3] together with this report, fulfill the OIG's reporting responsibilities under FISMA and related OMB guidance. We conducted this audit in accordance with generally accepted government auditing standards. Appendix I of this report discusses our audit objective, scope, and methodology in detail.

BACKGROUND

In fulfilling its legislative mandate of insuring deposits, supervising financial institutions, and managing receiverships, and in its role as a federal employer and acquirer of services, the FDIC creates and obtains a significant amount of PII related to depositors and borrowers at FDIC-insured financial institutions and FDIC employees and contractors. Implementing proper security controls over this PII 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 data security breaches at federal agencies have raised privacy concerns among federal agencies, the public, and the Congress and underscore the importance of implementing a strong, enterprise-wide privacy program.

Much of the PII managed by the FDIC and its contractors falls within the scope of several statutes and regulations intended to protect such information from unauthorized disclosure. These statutes and regulations include section 522 of the Consolidated Appropriations Act, 2005 (Division H of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005) (section 522); the Privacy Act of 1974; section 208 of the E-Government Act of 2002; and the FDIC's Rules and Regulations—Parts 309, *Disclosure of Information*, and 310, *Privacy Act Regulations*. In addition, OMB has issued a number of privacy-related memoranda containing policies and guidelines aimed at protecting PII at federal departments and agencies. The following summarizes the key OMB privacy-related memoranda included in our audit.

- **Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007**, requires agencies to develop and implement a breach notification plan and policy within 120 days.
- **Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006,** provides guidance to agencies for reporting security incidents involving PII and reminds agencies of existing requirements to protect PII.
- **Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006,** recommends that federal departments and agencies implement a

[3] KPMG report entitled, *Independent Evaluation of the FDIC's Information Security Program – 2007* (FDIC OIG Report No. AUD-07-014, dated September 27, 2007).

series of controls to safeguard the remote access, transport, and storage of sensitive information, including PII.

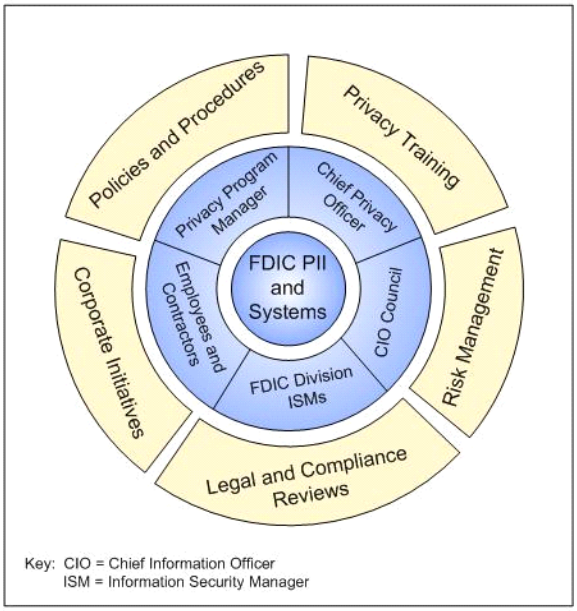
- **Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006,** re-emphasizes agency responsibilities to safeguard PII and train employees on their privacy responsibilities. The memorandum directs agencies to review their privacy policies and processes and take corrective action, as appropriate, to ensure adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, PII.
- **Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, dated February 11, 2005,** requests executive departments and agencies to designate a senior official with agency-wide responsibility for information privacy issues.
- **Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated September 26, 2003**, provides guidance to agencies on implementing the privacy provisions of the E-Government Act of 2002 and directs agencies to review the manner in which information on individuals is handled within agencies.

The extent to which these memoranda are legally binding on the FDIC varies. Similarly, the extent of the FDIC's voluntary compliance varies. Appendix II contains further information as well as a brief description of pertinent privacy-related laws, policies, and guidelines (including OMB memoranda) and their legal effect on the FDIC.

The FDIC's Privacy Program

The FDIC has established a corporate-wide privacy program to protect the PII it manages from unauthorized use, access, disclosure, or sharing and to safeguard associated information systems from unauthorized access, modification, disruption, or destruction. As illustrated in the figure, key components of the FDIC's privacy program include, but are not limited to, a Chief Privacy Officer (CPO) with overall responsibility for the program; a Privacy Program Manager who supports the CPO in developing and implementing privacy requirements; policies and procedures for managing and protecting PII; a process for identifying PII contained in applications; and procedures for conducting PIAs of applications and systems containing PII. The FDIC's privacy program also includes mandatory privacy-awareness training for employees and contractors, a Web site to provide information regarding privacy requirements, and targeted privacy briefings for personnel responsible for handling PII.

The FDIC's Privacy Program Components



Source: OIG analysis of the FDIC's Privacy Program.

In addition, the FDIC has placed bins and media consoles in its facilities to securely dispose of sensitive information (including PII), developed a standard privacy clause for its contracts, and conducted an initial assessment of FDIC contractors that access, maintain, or manipulate PII for the FDIC to determine the types of PII they possess and whether independent security reviews have been performed.

The FDIC recognizes that implementing effective measures to protect PII requires a sustained effort. Toward that end, the FDIC has designated privacy as an issue warranting special attention for 2007 in its annual assurance statement guidance to FDIC managers in support of the Federal Managers' Financial Integrity Act of 1982. Additionally, the FDIC recently hired a staff member to support its privacy program and plans to hire another staff member in the near future. Finally, the FDIC is conducting walk-throughs of its facilities to identify instances in which PII needs to be better secured and is integrating its key ongoing and planned privacy program control activities into a formal documented framework.

RESULTS OF AUDIT

The FDIC continues to take action to safeguard its PII and related systems and address privacy-related provisions of recent OMB memoranda. Of particular note, the FDIC has appointed a senior agency official for privacy, conducted privacy reviews prescribed by OMB,[4] and provided employees and contractors with privacy-awareness training. Importantly, the FDIC has established a process for conducting privacy impact assessments of its information systems containing PII that is consistent with relevant privacy-related policy, guidance, and standards. In addition, the FDIC is making satisfactory progress in implementing the provisions of OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006. Further, the FDIC is working to complete a number of ongoing privacy program initiatives to safeguard its PII and related systems consistent with privacy-related statutes, policies, and guidelines. Such initiatives include:

- Deploying new software that automatically encrypts sensitive information stored on portable computing devices, such as laptop computers, CDs/DVDs,[5] and USB[6] flash drives, as recommended in OMB Memorandum M-06-16. The FDIC is in the process of replacing its older encryption solutions that require manual

[4] OMB Circular No. A-130, *Management of Federal Information Resources;* Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*, requires agencies to conduct reviews of the following topics, at the indicated frequency: *Section (m) Contracts, Recordkeeping Practices, Privacy Act Training, Violations, and System of Records Notices*, every 2 years; *Routine Use Disclosures* and *Exemption of System of Records* reviews, every 4 years; and *Matching Programs*, annually.

[5] A Compact Disk and Digital Versatile Disk (CD/DVD) are optical digital disc formats used to store programs and data files.

[6] A Universal Serial Bus (USB) flash drive is a memory card that emulates a small disk drive and allows data to be easily transferred from one computer to another.

intervention by users, limiting assurance that sensitive information is consistently encrypted.[7]

- Conducting a comprehensive review of access controls over sensitive information stored on network shared drives throughout the Corporation to reduce the risk of unauthorized disclosure of sensitive information, including PII, consistent with the security principle of "least privilege."[8, 9]
- Ensuring that access to applications containing PII is limited consistent with the security principle of "least privilege."[10]
- Referencing in corporate policy the FDIC's new breach notification plan and procedures for responding to PII breaches.
- Implementing measures to ensure technologies used to collect, use, store, and disclose PII allow for continuous auditing[11] of compliance with stated privacy policies and practices as required by section 522.
- Logging all computer-readable data extracts from databases holding sensitive information and verifying that each extract, including sensitive data, has been erased within 90 days or its use is still required as recommended in OMB Memorandum M-06-16.

This report contains no recommendations. We plan to follow up on the status of these initiatives as part of privacy reviews conducted pursuant to section 522.

THE FDIC's PRIVACY IMPACT ASSESSMENT PROCESS

Section 208 of the E-Government Act of 2002, as implemented through OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, requires agencies to conduct PIAs of all information systems containing PII and make the completed PIAs generally available to the public. Section 208 requires that published PIAs describe, among other things, the information being collected, why the information is being collected, and the agency's intended use of the information. PIAs are intended to promote the public trust through increased transparency and assurances that personal information is properly protected.

---

[7] FDIC OIG report entitled, *Division of Resolutions and Receiverships Protection of Electronic Records* (Report No. AUD-07-010 dated September 2007), states that sensitive information, including PII, stored on portable computing devices was not being encrypted and that access to sensitive information, including PII, stored on network shared drives and network applications was not adequately restricted.

[8] OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, defines the term "least privilege" as the practice of restricting user access to only those IT resources (including data) needed to perform official duties.

[9] See footnote 7.

[10] See footnotes 7 and 8.

[11] In this context, continuous auditing refers to management's review of audit records (i.e., audit trails) for indications of inappropriate or unusual activity. Special Publication (SP) 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, issued by the National Institute of Standards and Technology (NIST) (a non-regulatory federal agency within the U.S. Department of Commerce) recommends that agencies configure their information systems to generate audit trails based on organization-defined auditable events and regularly analyze those audit trails.

OMB Memorandum M-07-19 directs agency IGs to assess the quality of their respective agency's PIA process, including the agency's adherence to privacy-related policy, guidance, and standards. In summary, we found that the FDIC's PIA process was satisfactory and consistent with relevant privacy-related policy, guidance, and standards. KPMG evaluated and reported on the adequacy of the FDIC's PIA process in its January 2007 audit report, *The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005*. KPMG concluded that the FDIC had established a formal process for conducting PIAs of its applications and systems containing PII and posting completed PIAs on its public Web site. However, KPMG noted that the FDIC's PIA process did not always ensure that publicly-posted PIAs contain sufficient information regarding the FDIC's collection or use of PII consistent with OMB policy and section 208 of the E-Government Act of 2002. KPMG recommended that the FDIC's CPO enhance the FDIC's PIA process and review all publicly-posted PIAs to determine whether they contain adequate disclosure regarding the types of PII used and the FDIC's use of PII.

In response to KPMG's recommendations, the CPO completed a review of all the PIAs posted on the FDIC's public Web site and made revisions, where warranted, to ensure that disclosures regarding the types of PII used in the PIAs were adequate and that descriptions of the FDIC's use of PII also were adequate. The CPO also strengthened the FDIC's PIA procedures by developing a PII checklist to be completed during the PIA process. Further, the FDIC added resources to its privacy program to help ensure that PIAs are thoroughly reviewed prior to being posted on the Web site.

THE FDIC'S PROGRESS IN IMPLEMENTING THE PROVISIONS OF OMB MEMORANDUM M-06-15

OMB Memorandum M-06-15 re-emphasizes agency responsibilities, under existing law and policy, to appropriately safeguard PII and train agency employees on their privacy responsibilities. Further, OMB Memorandum M-07-19 directs agency IGs to assess their agencies' (1) progress in implementing the provisions of OMB Memorandum M-06-15 since the most recent self-review, including an agency's policies and processes, (2) administrative, technical, and physical means used to control and protect PII. In summary, we concluded that the FDIC is making satisfactory progress in implementing the provisions of OMB Memorandum M-06-15. Table 1, on the next page, identifies selected key provisions of OMB Memorandum M-06-15 and summarizes the status of the FDIC's actions related to each of those provisions.

Table 1: Status of FDIC Actions Related to Selected Key Provisions of OMB Memorandum M-06-15

Selected Key Provisions	Status of FDIC Actions
The Senior Official for Privacy shall conduct a review of the agency's privacy program policies and processes and take corrective action, as appropriate, to ensure adequate safeguards are in place to prevent the intentional or negligent misuse of, or unauthorized access to, PII. The review must address all administrative, technical, and physical means used by the agency to control such information, including, but not limited to, procedures and restrictions on the use or removal of PII beyond agency premises or control.	The FDIC completed a review of its privacy program policies and Web sites on August 10, 2006. In addition, the FDIC has completed reviews of its compliance with various provisions of the Privacy Act of 1974 as required by OMB Circular No. A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*. Further, the FDIC's Division of Information Technology (DIT) established a process for periodically conducting walk-throughs of FDIC facilities to identify potentially vulnerable PII.
Agencies shall include any privacy weaknesses identified in security Plans of Action and Milestones (POA&M) already required by FISMA.	The FDIC reports its high-level, systemic privacy-related weaknesses to OMB in an agency-wide POA&M on an annual basis. The FDIC tracks and reports its other privacy program deficiencies and initiatives through various means, such as monthly status reports, a project plan, and the Internal Risks Information System (IRIS).[12] In addition, the FDIC is working to develop a formal, documented privacy program framework by December 15, 2007. The framework will document and describe the Corporation's privacy program goals and objectives, performance measures, organization and relationships of key initiatives, training and awareness strategy, and methods for reporting.

[12] IRIS is the FDIC's official tracking database for all U.S. Government Accountability Office and OIG audits and reviews of the FDIC and 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.

Selected Key Provisions	Status of FDIC Actions
Agencies shall remind their employees of their specific responsibilities for safeguarding PII, the rules for acquiring and using such information, and the penalties for violating these rules.	The FDIC sent a global e-mail message to all employees and contractors on August 8, 2006 reminding them of their responsibilities for safeguarding PII, the rules for acquiring and using such information, and the penalties for violating these rules. The CPO issued a follow-up global e-mail message on May 3, 2007, in conjunction with the issuance of FDIC Circular 1360.9, *Protecting Sensitive Information*, also dated May 3, 2007. The message again reminded all employees and contractors of their responsibilities regarding the protection of PII. In addition, the FDIC requires its employees and contractors to certify, on an annual basis, the completion of privacy-awareness training that addresses responsibilities for safeguarding PII, the rules for acquiring and using such information, and the penalties for violating those rules.
Agencies shall report security incidents to proper authorities, including IGs; other law enforcement; and in certain circumstances, the U.S. Department of Homeland Security.	The FDIC has established and implemented policy and procedures for reporting security incidents to proper authorities. In addition, the FDIC developed a breach notification plan and procedures in response to OMB Memorandum M-07-16.

STATUS OF THE FDIC'S ACTIONS TO ADDRESS SELECTED KEY PROVISIONS OF OMB PRIVACY-RELATED MEMORANDA

The FDIC has a number of initiatives underway to ensure its PII and related systems are safeguarded consistent with privacy-related statutes, policies, and guidelines. Table 2 below identifies selected key provisions of privacy-related memoranda recently issued by the OMB and the status of the FDIC's actions with regard to each of those provisions. We selected these provisions as being most germane to the reporting questions directed to senior agency privacy officials in section D of OMB Memorandum M-07-19 and to the FDIC's privacy program.

Table 2: Status of FDIC Actions to Address Selected Key Provisions of Privacy-related Memoranda Issued by the OMB

Selected Key Privacy Provisions of OMB Memoranda	Status of FDIC Actions
OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*	
PIA Processes. The agency conducts PIAs for electronic information systems and collections and, in	The FDIC has established and implemented a formal process for conducting PIAs of its applications and systems that contain PII. The FDIC posts its PIAs on

Selected Key Privacy Provisions of OMB Memoranda	Status of FDIC Actions
general, makes them available to the public.	its public Web site consistent with OMB policy and the E-Government Act of 2002.
Web Privacy Policies. The agency posts privacy policies on its public Web site(s).	The FDIC has posted a privacy policy describing its privacy practices (e.g., type of information collected, how the information is used, and who has access to the information) on its public Web site.
Machine-readable Policies. The agency translates privacy policies into a standardized machine-readable format.	The FDIC's public Web site contains machine-readable Web site policies.
Persistent Tracking Technology. The agency prohibits the use of persistent tracking technology (i.e., cookies) or any other means (e.g., Web beacons[13]) to track visitors' activity on the Internet, except when properly approved by a senior agency official due to a compelling need.	The FDIC uses persistent tracking technology for two of its applications: the Statistics on Depository Institutions and FDIC*connect*.[14] In both cases, the use of persistent tracking technology is approved in writing by the CPO. In addition, the FDIC has in place a DIT policy regarding the use of persistent tracking technology. The FDIC is drafting a similar corporate policy to ensure compliance with the policy among all divisions of the FDIC.
OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*	
Senior Agency Officials for Privacy. The Agency designates a senior official who has overall, agency-wide responsibility for information privacy issues.	The FDIC has designated the CPO as the senior agency official for privacy; the CPO has overall agency-wide responsibility for information privacy issues. The FDIC has also designated a Privacy Program Manager to assist the CPO in implementing the FDIC's privacy program. Further, the FDIC has hired one additional staff member and is in the process of filling a remaining position to support the privacy program.
OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*	
Encryption of Sensitive Data on Mobile Computing Devices. The agency encrypts all data on mobile	The FDIC is in the process of replacing its older laptop encryption solutions that require manual intervention by users, limiting management's assurance that

[13] A Web beacon is often a transparent graphic image, placed on a Web site or in an e-mail, that is used to monitor the behavior of users visiting the Web site or sending e-mails. Web beacons are typically used by a third party to monitor the activity of a site.

[14] Statistics on Depository Institutions is an advanced feature of the FDIC's Institution Directory that allows users to obtain more detailed financial reports and provides the ability to create reports. FDIC*connect* is a secure Web site for insured financial institutions to conduct E-commerce with the FDIC.

Selected Key Privacy Provisions of OMB Memoranda	Status of FDIC Actions
computing devices that carry agency data, unless the data are determined, in writing, to be non-sensitive.	sensitive information is consistently encrypted. The new software being deployed automatically encrypts sensitive information stored on corporate laptop computers. The deployment of the new encryption software was approximately 60 percent complete at the end of August 2007 and is expected to be completed by the end of September 2007. Following the rollout of the new laptop encryption software, the FDIC plans to identify and deploy new software that automatically encrypts information stored on removable media, such as CDs/DVDs, USB flash drives, and personal digital assistants. The FDIC's current encryption solutions for removable media also require manual intervention by users, limiting management's assurance that sensitive information is consistently encrypted on mobile computing devices. The FDIC does not currently encrypt back-up tapes that contain sensitive information. According to an FDIC privacy official, the FDIC has investigated available encryption solutions for securing tape media and has not found a solution that works across the FDIC environment. This is an area that the FDIC will continue to explore following its encryption efforts for other portable media.
Remote Access with Two-Factor Authentication. Allow remote access only with two-factor authentication,[15] whereby one of the factors is provided by a device separate from the computer gaining access.	The FDIC requires that two factors be used when remote users authenticate to the FDIC's network. However, in some cases, the FDIC's implementation of two-factor authentication for remote access does not satisfy OMB's definition of two-factor authentication because the second factor is not "a device separate from the computer gaining access."
Remote Access Time-Out. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity.	Generally, the FDIC requires that remote users of its network re-authenticate after 15 minutes of inactivity. However, there are circumstances in which remote users are not required to re-authenticate to the network after 30 minutes of inactivity.
Data Extract Logging and 90-Day Deletion. Log all computer-readable data extracts from databases holding sensitive information, and verify that	The FDIC is researching potential software solutions that will log all computer-readable data extracts from databases holding sensitive data.

[15] According to NIST SP 800-53 Rev. 1, *Recommended Security Controls for Information Systems*, authentication of user identities is accomplished through the use of passwords; tokens; biometrics; or in the case of multifactor authentication, some combination thereof.

Selected Key Privacy Provisions of OMB Memoranda	Status of FDIC Actions
each extract, including sensitive data, has been erased within 90 days or its use is still required.	
NIST Security Checklist. The agency implements a checklist, developed by NIST, to protect PII that is accessed remotely or physically transported outside an agency's secured physical perimeter. The intent of the controls contained in the checklist is to compensate for the lack of physical security controls when information is removed or accessed from outside an agency's facilities.	DIT plans to confirm that the control measures described in the NIST checklist are effectively implemented through its ongoing and planned security testing and evaluation of information systems. The FDIC performed risk assessments of its major applications and general support systems prior to the final publication of NIST SP 800-53 in February 2005. At the time the risk assessments were conducted, the FDIC was planning to perform separate, streamlined risk assessments of its non-major information systems that process sensitive information (including PII) in support of system security certification and accreditation. In the spring of 2006, the FDIC decided to forgo that approach and, instead, aggregate its non-major applications into a major application or general support system to achieve efficiencies in its certification and accreditation practices. To the extent that non-major information systems processing PII are included in the aggregation, further risk assessments and security testing and evaluation may be required, and additional control measures may be necessary to ensure that remote access, transport, and storage of PII are properly safeguarded.
M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*	
The agency reports all incidents involving PII to the U.S. Computer Emergency Readiness Team (US-CERT) within 1 hour of discovering the incident.	FDIC Circular 1360.9, *Protecting Sensitive Information*, states that the FDIC's Computer Security Incident Response Team shall notify the US-CERT within 1 hour of an incident if the incident involves the loss or compromise of PII. This circular also requires (1) immediate reporting of an event in which sensitive data are suspected or known to be lost or otherwise compromised to the DIT Help Desk and (2) notification be made to the supervisor/oversight manager and division/office Information Security Manager at the earliest opportunity. In addition, the FDIC prepared a breach notification plan and procedures for responding to PII breaches in response to OMB Memorandum M-07-16.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*	
Breach Notification Policy. The agency implements a breach notification policy consistent with OMB Memorandum M-07-16 and prior OMB memoranda. The policy is to be implemented within 120 days of the date of the OMB memorandum (i.e., not later than September 19, 2007).	The FDIC is currently working to augment its corporate breach notification policy with procedures for responding to PII breaches. The procedures address certain matters, outlined in OMB Memorandum M-07-16, that are not in current FDIC policy, such as privacy requirements for reporting and handling PII breaches and external notifications on such breaches.
Reducing PII. To reduce the risk of a breach of PII, the agency reduces the volume of collected and retained PII to the minimum necessary.	The CPO initiated a remediation project in 2005 to assess the use and protection of SSNs and employee identification numbers in the FDIC's information systems. This project includes reducing the use of PII in FDIC systems, wherever practical, to reduce the risk of a breach of PII. This project is ongoing.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of the audit was to assess the status of the FDIC's privacy program activities and initiatives. Our work focused on the status of the FDIC's efforts to address selected key provisions of privacy-related memoranda recently issued by OMB. As part of our work, we followed up on privacy-related issues identified in prior audit reports as detailed in the *Audit Coverage* section below. Additionally, the OIG contracted separately with KPMG to conduct a performance audit of the FDIC's information security program and practices pursuant to FISMA. As part of its security program evaluation, KPMG prepared responses to security-related questions directed to agency IGs in OMB Memorandum M-07-19. KPMG's security program evaluation report,[16] together with this report, fulfill the FDIC OIG's reporting responsibilities under FISMA and related OMB guidance.

We performed the audit at the FDIC's offices in Arlington, Virginia, from June through August 2007. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Methodology

To accomplish the objective, we interviewed key FDIC officials with privacy responsibilities, including the Chief Information Security Officer and Privacy Program Manager. Additionally, we reviewed relevant laws and regulations and the FDIC's privacy program policies, procedures, and guidance. We also reviewed key privacy-related documentation, including PIAs, status reports, privacy-awareness training materials, approvals for the use of persistent tracking technology, privacy-related reviews performed by the FDIC, and the FDIC's breach notification plan and procedures.

Audit Coverage

As a part of our current audit, we followed up on privacy-related issues identified in prior audit reports, particularly KPMG's January 2007 report, *The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005* (Report No. 07-003). We considered the results of these prior and current audits in planning and conducting our audit work:

- FDIC OIG Audit Report No. 06-018, *Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and*

[16] KPMG Report No. AUD-07-014 , *Independent Evaluation of the FDIC's Information Security Program – 2007, dated September 2007.*

Agency Privacy Management, dated September 22, 2006.

- FDIC OIG Audit Report No. 06-020, *The FDIC's Efforts to Comply with OMB Memorandum M-06-16, Protection of Sensitive Agency Information*, dated September 25, 2006.
- FDIC OIG Audit Report No. 07-003, *The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005*, dated January 10, 2007.
- OIG Audit Report No. 07-010, *Division of Resolutions and Receiverships Protection of Electronic Records*, dated September 2007.
- KPMG Report No. AUD-07-014, *Independent Evaluation of the FDIC's Information Security Program – 2007*, dated September 2007.

Compliance With Laws and Regulations

Our assessment of compliance with laws and regulations was limited to the portions of statutes directly related to the FISMA reporting instructions on assessments to be performed by the IGs. Specifically, we evaluated whether the FDIC had established processes for conducting PIAs as required by the E-Government Act of 2002. Our audit also assessed the FDIC's progress in implementing PII safeguards recommended in OMB memorandum M-06-15, *Safeguarding Personally Identifiable Information*, which reemphasizes agency responsibilities under law, in particular the Privacy Act of 1974. Appendix II contains information regarding privacy-related laws, policies, and guidelines.

Reliance on Computer-based Data, Government Performance and Results Act, and Fraud and Illegal Acts

Our audit objective was limited to assessing the status of the FDIC's privacy program activities and initiatives. Accordingly, to answer our audit objective, we did not consider it necessary to develop procedures to assess the reliability of computer-based data or privacy program performance measures. In addition, we did not design specific audit procedures to detect fraud; however, throughout the audit, we were sensitive to the potential for fraud and illegal acts. No indications of fraud or illegal acts came to our attention during the audit.

APPENDIX II

PRIVACY-RELATED LAWS, POLICIES, AND GUIDELINES

A number of federal statutes, policies, and guidelines are aimed at protecting (1) PII from unauthorized use, access, disclosure, or sharing and (2) associated information systems from unauthorized access, modification, disruption, or destruction. Brief descriptions of key privacy-related statutes, policies, and guidelines and their legal effect on the FDIC follow.

The Privacy Act of 1974 (http://www.usdoj.gov/oip/privstat.htm)
Imposes various requirements for federal agencies whenever they collect, create, maintain, and distribute records (as defined in the Act, and regardless of whether they are in hardcopy or electronic format) that can be retrieved by the name of an individual or other identifier. One such requirement is to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained. The Act also prohibits releasing data on individuals without their permission, subject to various exceptions. Moreover, the Act requires agencies to publish the *Federal Register* notices that describe the systems of records the agencies maintain on individuals. As a federal agency, the FDIC is subject to the requirements of the Act.

The Paperwork Reduction Act of 1995 (http://www.archives.gov/federal-register/laws/paperwork-reduction/)
Requires the Director of OMB to develop policies that protect the privacy of the information maintained by agencies (including the FDIC). See the discussions of OMB Circulars and memoranda that follow.

The E-Government Act of 2002, (http://www.cio.gov/archive/e_gov_act_2002.pdf)
Seeks to promote electronic government services and to enhance access to government information consistent with laws regarding personal privacy. Section 207 of the Act is intended to improve the methods by which government information, including information on the Internet, is organized, preserved and made accessible to the public. Section 208 is intended to protect personal information by requiring agencies to (1) conduct PIAs of information systems and collections and, in general, make PIAs publicly available; and (2) report annually to the OMB on compliance with section 208. The Act also requires the Director, OMB to draft guidelines regarding (1) agency posting of privacy policies on agency Web sites used by the public; and (2) translate privacy policies into a machine-readable format. The FDIC has determined that it is subject to the requirements of this provision. Refer to FISMA legislation for additional information.

Federal Information Security Management Act of 2002 (FISMA) (title III of the E-Government Act of 2002) (http://csrc.nist.gov/policies/FISMA-final.pdf)
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.

Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of the Consolidated Appropriations Act, 2005) (http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ447.108.pdf (See page 460 of 658))
Requires, among other things, that agencies protect PII, designate a CPO, conduct PIAs under appropriate circumstances, report to the Congress and agency IG on privacy matters, and provide training to employees on privacy and data protection policies. Section 522 also requires that every 2 years, the agency IG contract with an independent third party to conduct a review of the agency's privacy program and practices and that the IG issue a report based on that review. The FDIC has determined that section 522 of the Act applies to the Corporation.

APPENDIX II

Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*
(http://csrc.nist.gov/publications/fips/fips199/FIPSPUB- 199-final.pdf)
Describes standards to be used by all federal agencies to categorize all information and information systems collected or maintained by, or on behalf of, each agency based on the objectives of providing appropriate levels of information security according to a range of impact levels. This publication establishes security categorization standards for information and information systems based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. By its terms, this publication is not legally binding on the FDIC, but the FDIC intends to follow its principles.

FIPS PUB *200, Minimum Security Requirements for Federal Information and Information Systems* (http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf)
Specifies minimum security requirements for federal information and information systems supporting the executive agencies of the federal government in 17 security-related areas. The 17 areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems. An agency must determine information system level impacts under the FIPS PUB 199 standard prior to considering the minimum security requirements and appropriate security controls under the FIPS PUB 200 standard. The FDIC has determined that the minimum requirements of this publication are reasonable best practices which the FDIC should seek to follow.

NIST SP[17] 800-53 Rev. 1, *Recommended Security Controls for Information Systems*
(http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf)
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.

NIST SP 800-60, Volume I: *Guide for Mapping Types of Information and Information Systems to Security Categories* (http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf)
Contains basic guidelines for mapping types of information and information systems to security categories. This guidance maps identification types to the security categories and objectives and impact levels that are defined in FIPS PUB 199.

NIST SP 800-60, Volume II: *Guide for Mapping Types of Information and Information Systems to Security Categories* (http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf)
Contains the appendixes, including examples of impact assignments and security categorization rationale. This volume is to be used in conjunction with NIST 800-60 Volume I.

NIST SP 800-64, *Security Considerations in the Information Systems Development Life Cycle* (http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf)
Provides a framework for incorporating security into all phases of the information system development life cycle process, from initiation to disposal. Included within the framework are requirements to consider privacy protection measures in accordance with relevant privacy-related federal guidance.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
(http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

[17] NIST Special Publications contain guidelines or best practices that agencies should consider. These publications are not legally binding on the FDIC, but the FDIC's policy is, in general, to comply with them voluntarily.

Provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The publication also provides information on the selection of cost-effective security controls. Such controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information.

OMB Circular No. A-130, ***Management of Federal Information Resources***
(http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf)
Establishes policy for the management of federal information technology. The circular contains two relevant appendixes:

> **Appendix I,** ***Federal Agency Responsibilities for Maintaining Records About Individuals***, describes agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974. The head of each agency shall ensure that the following reviews are conducted: section (m) contracts (i.e., whereby agencies contract-out systems of records to accomplish an agency function); recordkeeping practices; routine use disclosures; exemption of systems of records; matching programs; Privacy Act training; violations; and systems of records notices. The FDIC has determined that OMB Circular No. A-130, Appendix I, applies to the Corporation.
>
> **Appendix III,** ***Security of Federal Automated Information Resources***, requires agencies to establish controls to assure adequate security for all information processed, transmitted, or stored in federal automated information systems. OMB A-130 Appendix III defines adequate security as security commensurate with the risk and magnitude of harm resulting from the loss; misuse; or unauthorized access to, or modification of, information. Most of the Circular's provisions are legally binding on the FDIC.

OMB Memorandum M-03-22, ***OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*** (http://whitehouse.gov/omb//memoranda/m03-22.html)
Provides detailed guidance to agencies on how to implement section 208 of the E-Government Act, see above. It provides definitions and explains when PIAs are or are not required, the manner in which PIAs are conducted, and their relationship with the Paperwork Reduction Act and the Privacy Act. The memorandum contains requirements for agency website, specifically regarding privacy policies and persistent tracking technologies ("cookies"). Other provisions address privacy policies in machine readable formats, responsibilities of agency officials, and reporting requirements. To the extent that the provisions of this memorandum are legally binding on the FDIC, the FDIC has taken steps to implement those provisions or has otherwise taken them into account.

OMB Memorandum M-05-08, ***Designation of Senior Agency Officials for Privacy***
(http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf)
Requests that agencies designate a senior official for privacy. The FDIC complied with the memorandum by designating the CPO as the senior agency official.

OMB Memorandum M-06-15, ***Safeguarding Personally Identifiable Information***
(http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf)
Describes responsibilities and the policy for appropriately safeguarding sensitive PII and for training employees on their responsibilities in this area. OMB requires the senior agency official for privacy to conduct a review of policies and processes and take corrective action as appropriate to ensure adequate safeguards exist to prevent misuse or authorized access to PII. Any weaknesses are to be identified in a security POA&M consistent with FISMA. According to the FDIC, to the extent that the provisions of OMB Memorandum M-06-15 are legally binding on the FDIC, the FDIC has taken steps to implement those provisions or has otherwise taken them into account.

APPENDIX II

OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
(http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf)
Includes a checklist for agency use in protecting PII that is remotely accessed or transported outside the agency. The checklist is based on NIST SPs 800-53, *Recommended Security Controls for Federal Information Systems;* and 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft). In addition, M-06-16 recommends the encryption of all data on mobile computers/devices that carry sensitive data, two-factor authentication for remote access, "time-out" functions for remote access and mobile devices, and the logging of all computer-readable data extracts from databases containing sensitive information. According to the FDIC, to the extent that the provisions of OMB Memorandum M-06-16 are legally binding on the FDIC, the FDIC has taken steps to implement those provisions or has otherwise taken them into account.

OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
(http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-19.pdf)
Provides guidance on the reporting of security incidents involving PII. This guidance requires all agencies to report all suspected or confirmed breaches involving PII in an electronic or physical form, within 1 hour of discovering the incident, to the U.S. Center Emergency Readiness Team, a federal incident response center located within the U.S.Department of Homeland Security. According to the FDIC, to the extent that the provisions of OMB Memorandum M-06-19 are legally binding on the FDIC, the FDIC has taken steps to implement those provisions or has otherwise taken them into account.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf)
Reiterates the need for agencies to comply with NIST standards and guidelines in connection with system certifications and accreditations and to train employees on privacy and security responsibilities. In addition, OMB Memorandum M-07-16 requires agencies to review and reduce the volume of PII and the use of SSNs in their records and to implement five security requirements from M-06-16 (see above). Newly added is the requirement for agencies to develop and implement a policy by September 19, 2007 for notifying third parties of security breaches involving PII. The FDIC will voluntarily comply with the provisions in Memorandum M-07-16.

OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf)
Provides instructions for meeting the reporting requirements under FISMA for fiscal year 2007. The memorandum also includes instructions for reporting the status of the privacy management program. It is the FDIC's practice to comply with the OMB's FISMA instructions.

FDIC Rules and Regulations

Part 309, *Disclosure of Information* (http://www.fdic.gov/regulations/laws/rules/2000-3800.html) sets forth the basic policies of the FDIC regarding the information it maintains and the procedures for obtaining access to such information.

Part 310, *Privacy Act Regulations*, (http://www.fdic.gov/regulations/laws/rules/2000-3900.html) establishes regulations implementing the Privacy Act of 1974 by delineating the procedures that an individual must follow in exercising his or her access or amendment rights under the Privacy Act of 1974 to records maintained by the Corporation in its systems of records, as defined in the Act.

FDIC Circular 1023.1, *Procedures for Processing Freedom of Information Act Requests*
(http://fdic01/division/doa/adminservices/records/directives/1000/1023-1.doc)
Contains the FDIC's procedures for processing requests and appeals pursuant to the Freedom of Information Act.

APPENDIX II

FDIC Circular 1031.1, *Administration of the Privacy Act*
(http://fdic01/division/doa/adminservices/records/directives/1000/1031-1.doc)
Establishes requirements for the collection, maintenance, use, and dissemination of records subject to the Privacy Act of 1974.

FDIC Circular 1360.9, *Protecting Sensitive Information*
(http://fdic01/division/doa/adminservices/records/directives/1000/1360-9.doc)
Establishes FDIC policy on protecting sensitive information collected and maintained by the Corporation and provides guidance for safeguarding the information.

FDIC Circular 1360.12, *Reporting Computer Security Incidents*
(http://fdic01/division/doa/adminservices/records/directives/1000/1360-12.doc)
Establishes FDIC policy on reporting suspected computer security incidents affecting all FDIC automated information systems resources to the FDIC Computer Security Incident Response Team.

FDIC Circular 1360.16, *Mandatory Information Security Awareness Training*
(http://fdic01/division/doa/adminservices/records/directives/1000/1360-16.doc)
Establishes FDIC policy on mandating annual information security awareness training for all employees and contractors who are involved in the management, use, or operation of a federal computer system within or under the supervision of FDIC.

Division of Information Technology IT Policy Memorandum, *Cookies in Internet Product* (http://fdic01.prod.fdic.gov/division/dit/cookies.html)
Establishes the policy and standard for the use of cookies in Internet, FDICnet, and extranet-type products developed or deployed by the FDIC.