



Office of Inspector General

May 2005
Report No. 05-018

Implementation of E-Government Principles

AUDIT REPORT

Office of Audits





Implementation of E-Government Principles

Results of Audit

Background and Purpose of Audit

E-Government is generally defined as the use of Internet-based technologies by government agencies to provide information and services to citizens, businesses, and other governmental agencies. In 2001, the President initiated several government reform efforts, collectively known as the President's Management Agenda (PMA), to make the federal government more results-oriented, efficient, and citizen-centered.

Expanded E-Government is one initiative in the PMA. The goals of the PMA and E-Government initiatives are to eliminate redundant systems and significantly improve the government's quality of customer service for citizens and businesses. The Office of Management and Budget (OMB) is using its Executive Branch Management Scorecard (Scorecard) to measure agency success in executing E-Government initiatives.

The original audit objective was to determine whether the FDIC (1) adequately implemented E-Government principles in its operations and information exchange with insured financial institutions and (2) complied with applicable portions of Government Paperwork Elimination Act. However, we limited our work to obtaining an understanding of the FDIC's progress on E-Government initiatives because the FDIC had not yet developed a comprehensive E-Government strategic plan.

The FDIC has made progress in implementing various initiatives that are consistent with E-Government principles and implementing guidance from OMB. In addition, the Corporation has taken steps to develop a comprehensive E-Government strategic plan that will be linked to associated corporate goals and objectives in areas addressed by OMB's Scorecard and the E-Government Act guidance. Absent such a strategic plan, with appropriate linkages to corporate goals and objectives, the FDIC risked not efficiently and effectively planning, coordinating, and implementing E-Government initiatives.

During our review, the Corporation established a Corporate Performance Objective in December 2004 to develop and implement a new E-Government strategy. The strategy will promote a paperless corporate environment in which the majority of transactions and data and document storage are handled electronically. The FDIC also established a working group that has developed a draft project plan to guide development of the E-Government strategic plan. At this time, the draft project plan does not specifically address either performance measures or desired outcomes for the E-Government initiatives.

After we completed our review, the Corporation established a milestone of December 31, 2005 for the approval of a new E-Government strategic plan.

Recommendations and Management Response

The actions taken by the Corporation during and after our review, together with planned actions, adequately address our finding. Thus, we are not making any recommendations. We suggest, however, that in completing the new E-Government strategic plan, the Corporation be mindful of OMB's guidance that E-Government performance measures must be linked to the Corporation's Annual Performance Plan and Strategic Plan and desired outcomes of E-Government initiatives must be identified.

Expanded E-Government Areas Monitored by OMB

- Establishment of an Enterprise Architecture
- Preparation of Business Cases for Major Systems Investments
- Remediation of Security Weaknesses
- Certification and Accreditation of Systems
- Establishment of a Process and Plan for Implementing E-Government Initiatives

Source: OMB's Scorecard.


TABLE OF CONTENTS

BACKGROUND	1
RESULTS OF AUDIT	4
THE FDIC'S PROGRESS IN IMPLEMENTING E-GOVERNMENT	4
Enterprise Architecture	4
Business Cases for Major Systems Investments	6
Remediation of Security Weaknesses	6
Certification and Accreditation of Systems	7
Other Corporate Efforts to Promote E-Government	8
Process and Plan for Implementing E-Government Initiatives	9
Conclusion	10
CORPORATION COMMENTS AND OIG EVALUATION	11
APPENDIX I: OBJECTIVE, SCOPE, AND METHODOLOGY	12
APPENDIX II: EXPANDED ELECTRONIC GOVERNMENT	14
FIGURE	
The FDIC's Enterprise Architecture Framework	5



DATE: May 24, 2005

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



FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *Implementation of E-Government Principles*
(Report No. 05-018)

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) has completed an audit of FDIC's implementation of E-Government principles. The objective of our audit was to determine whether the FDIC (1) adequately implemented E-Government principles in its operations and information exchange with FDIC-insured financial institutions and (2) complied with applicable portions of the Government Paperwork Elimination Act (GPEA). As discussed in detail in Appendix I, we limited the scope of our audit to obtaining an understanding of the Corporation's progress on E-Government initiatives after we determined that the FDIC had not developed an E-Government strategic plan.

BACKGROUND

E-Government is generally defined as the use of Internet-based technologies by government agencies to provide information and services to citizens, businesses, and other governmental agencies. E-Government initiatives are increasingly being leveraged as technological advancements and rising citizen expectations set a standard for a more accessible, reliable, and streamlined government. Further, E-Government has been the subject of initiatives established and guidance issued by the President and the Office of Management Budget (OMB) and in legislation passed by the Congress in December 2002. The initiatives, guidance, and legislation, which are not always applicable to the FDIC, represent prudent business practices (see discussion of applicability in Appendix I).

President's Management Agenda

In 2001, the President initiated several government reform efforts, collectively referred to as the President's Management Agenda (PMA), to make the federal government more results-oriented, efficient, and citizen-centered. The PMA includes five broad initiatives:

- Human Capital
- Competitive Sourcing
- Improving Financial Performance

- Expanded E-Government
- Budget and Performance Integration

The goal of the PMA and E-Government initiatives is to eliminate redundant systems and significantly improve the government's quality of customer service for citizens and businesses. E-Government initiatives are (1) citizen-centered rather than bureaucratic or agency-centered, (2) results-oriented by producing measurable improvements for citizens, and (3) market-based by actively promoting innovation.

OMB E-Government Strategy

In February 2002, OMB issued the *E-Government Strategy*, designating 24 high-profile initiatives to lead the government's transition to E-Government. The 24 initiatives are divided among 4 key portfolios:

- **Government to Citizen** initiatives provide one-stop, on-line access to information and services to citizens.
- **Government to Business** initiatives help business interact efficiently and effectively with the federal government.
- **Government to Government** initiatives forge new partnerships among levels of government. These partnerships should also facilitate collaboration between levels of government and empower state and local governments to deliver citizen services more effectively.
- **Internal Efficiency and Effectiveness** initiatives apply industry's best practices to government.

E-Government Act of 2002

The President signed the E-Government Act of 2002 (Act) on December 17, 2002; most of the Act's provisions became effective on April 17, 2003. The purpose of the Act was to enhance the management and promotion of electronic government services and processes by establishing a federal Chief Information Officer (CIO) within the OMB and by establishing a broad framework of measures that require using Internet-based information technology (IT) to enhance citizen access to government information and services. The Act, in essence, codified the PMA, added new initiatives to previously established statutory requirements, and required federal agencies to follow OMB guidance on E-Government.

OMB E-Government Act Guidance

In August 2003, OMB issued guidance on specific actions required under the Act. Specifically, according to *Implementation Guidance for the E-Government Act of 2002*, agencies are expected to do the following:

- **Define and deliver performance increases that matter to citizens** – Agencies are to develop performance measures for E-Government that are both citizen- and productivity-related. The measures must be linked to the agency’s Annual Performance Plan and Strategic Plan and be used to meet agency objectives, strategic goals, and statutory mandates in E-Government and IT.
- **Communicate policies within and across agencies** – The agency CIO will serve as the primary official for assisting agency heads in implementing the Act and OMB guidance.
- **Comply with section 508 to ensure accessibility** – Agencies are to continue to comply with section 508 of the Rehabilitation Act of 1973.¹

Other agency requirements include: making public regulations and rulemaking processes electronically accessible, conducting assessments of effects on privacy issues in relation to new IT investments and on-line information collections, and establishing and operating IT training programs for personnel.

OMB Executive Branch Management Scorecard

The OMB Executive Branch Management Scorecard (Scorecard) tracks how well the departments and major agencies are executing the five PMA initiatives. The OMB Scorecard employs a simple stoplight scoring system common today in well-run businesses, using green for success, yellow for mixed results, and red for unsatisfactory results.

With regard to expanded E-Government, OMB is monitoring progress in the following areas to measure agencies’ success.

- Establishment of an Enterprise Architecture
- Preparation of Business Cases for Major Systems Investments
- Remediation of Security Weaknesses
- Certification and Accreditation of Systems
- Establishment of a Process and Plan for Implementing E-Government Initiatives

The specific standards for the expanded E-Government element of the Scorecard are in Appendix II. As of December 31, 2004, the OMB Scorecard showed that many of the departments and major agencies are making progress toward implementing the initiatives.

¹ The FDIC is not required by law to comply with the provisions of the Rehabilitation Act of 1973 but does voluntarily comply.

The FDIC's Division of Information Technology and CIO Council

The FDIC's Division of Information Technology (DIT) has overall responsibility for the Corporation's IT activities and the E-Government initiatives. Also, the FDIC has established a CIO Council to advise the CIO on all aspects of adoption and use of IT at the FDIC. The Council has taken a leadership role in developing a strategy for and implementing the Corporation's E-Government initiatives.

RESULTS OF AUDIT

The FDIC had made progress in implementing various initiatives that are consistent with E-Government principles and implementing guidance from OMB. In addition, the Corporation had taken steps to develop a comprehensive E-Government strategic plan that will be linked to associated corporate goals and objectives in areas addressed by OMB's Scorecard and the E-Government Act guidance. Absent such a strategic plan, with appropriate linkages to corporate goals and objectives, the FDIC risked not efficiently and effectively planning, coordinating, and implementing E-Government initiatives.

THE FDIC'S PROGRESS IN IMPLEMENTING E-GOVERNMENT

The FDIC had issued an IT strategic plan, had developed a high-level E-Government Strategy, and implemented, or was in the process of implementing, activities and information systems that were consistent with E-Government principles and that addressed PMA initiatives. However, the Corporation had not developed a comprehensive E-Government strategic plan that included, or that was linked to, goals and objectives in areas outlined in the E-Government Act. Further, the Corporation had not finalized a process to implement appropriate E-Government initiatives. As a result, the FDIC risked not efficiently and effectively implementing the initiatives.

Enterprise Architecture

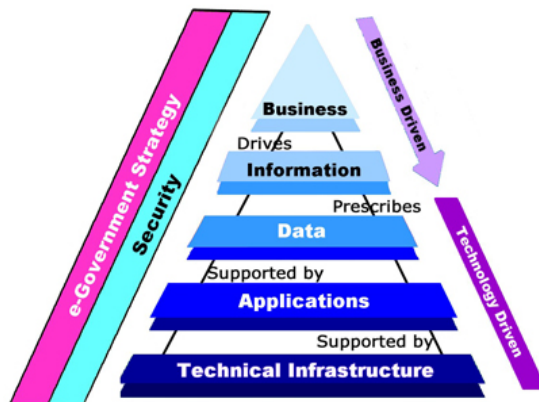
Development of agency enterprise architectures will assist in building a comprehensive business-driven blueprint of the entire federal government. The development of this framework has and will continue to enable the federal government to identify opportunities to leverage technology; reduce redundancy; facilitate information sharing; establish a direct relationship between IT and mission/program performance; and maximize IT investments to better achieve mission outcomes.

Source: OMB's Expanding E-Government Results Report.

During 2002, the FDIC began developing an enterprise architecture (EA) to establish a corporate-wide roadmap for achieving the FDIC's mission within an efficient IT

environment. The FDIC's E-Government strategy is a component of the EA that focuses on service delivery for the FDIC's internal and external customers. The FDIC's EA Framework is shown below.

The FDIC's Enterprise Architecture Framework



Source: The FDIC's DIT.

The FDIC had taken the following actions in developing and implementing an EA:

- Developed an EA Blueprint that defines, at a high level, the FDIC's current and target EAs, including a security architecture.
- Drafted a Security Standards Profile that identifies the security standards specific to the security services specified in the EA.
- Established a Technical Review Group for reviewing new and upgraded IT security solutions.
- Developed an EA Technical Reference Model that identifies and describes security services throughout the Corporation.
- Created checklists to facilitate the analysis of information security associated with IT investments.
- Issued formal policies for the FDIC's EA and Capital Planning and Investment Management programs.
- Continued the oversight of EA products and processes and evaluated proposed IT investments for alignment with the information security architecture principles contained in the EA Blueprint.
- Initiated a pilot implementation of an EA Repository product to integrate EA-related products and information currently housed in various FDIC systems and data sources and establish an automated, comprehensive, accurate, and dynamic baseline for the EA.
- Implemented an on-line publication, *The Architect*, to communicate news and information related to the EA program internally for FDIC employees.

Business Cases for Major Systems Investments

Business cases have clearly defined vision and outcomes, including security linked to the department's or agency's mission through their enterprise architecture with benefits far outweighing the costs.

Source: OMB's Expanding E-Government Results Report.

The FDIC had established a Capital Investment Review Committee (CIRC) that reviews all IT initiatives with capital outlays of more than \$3 million. The CIRC also reviews certain other projects that cost less but are considered critical to the FDIC. The CIRC determines whether a proposed investment is appropriate for consideration by the FDIC Board of Directors and oversees approved investments throughout their life cycle. The FDIC Capital Investment policy requires an executive sponsor for each IT capital investment to be responsible for establishing a link between the recommended investment and the FDIC's strategic goals and objectives. Further, the policy requires project teams to develop a project proposal (i.e., a business case) that documents the business needs of the project. Among other things, the business case must demonstrate financial soundness and alignment with the EA and provide support for the organization's business needs and the users' needs.

In February 2004, the FDIC created the CIO Council as one of the primary governance mechanisms for IT management. The CIO Council is composed of senior IT-focused executives from each of the FDIC's business line divisions. The Council is responsible for advising the CIO in developing an enterprise perspective on corporate systems; assisting in the development of an overall IT strategic plan; and reviewing IT initiatives, projects, priorities, and resources. The CIO Council is responsible for setting the strategic direction for IT and, in concert with the CIRC, is responsible for reviewing and recommending IT investments by the Corporation.

Remediation of Security Weaknesses

Agency submits quarterly status reports to OMB regarding remediation of IT security weaknesses, and the Inspector General verifies the effectiveness of the security remediation process.

Source: Expanded Electronic Government Scorecard Criteria.

The FDIC uses the Internal Risks Information System (IRIS) as its primary management tool for monitoring and tracking the remediation of agency information security weaknesses. Specifically, the FDIC uses IRIS to monitor and track the resolution of Government Accountability Office and FDIC Office of Inspector General audits, reviews, evaluations, and surveys. The system contains Plans of Action and Milestones (POA&M) information (including findings, conditions, recommendations, corrective actions, and milestones) related

to information security weaknesses and tracks this information by audit, review, and evaluation. The FDIC assigned the Office of Enterprise Risk Management (OERM) primary responsibility for administering IRIS. The FDIC's divisions and offices, in coordination with OERM, are responsible for maintaining current, accurate, and complete information in IRIS for their respective business areas. OERM uses IRIS to generate periodic progress reports and briefings to FDIC management on the status of agency information security weaknesses.

The CIO is providing OMB with quarterly POA&M reports on the FDIC's progress in correcting its program-level security weaknesses. In August 2004, the FDIC began preparing system-level POA&Ms for its major applications and general support systems² to track security weaknesses identified through self-assessment reviews. We noted in our 2004 Federal Information Security Management Act (FISMA) evaluation report that we were not able to perform sufficient testing to fully evaluate the system-level POA&Ms because they had been recently implemented. We plan to perform a more detailed analysis of the FDIC's system-level POA&Ms as part of our 2005 FISMA evaluation work.

Certification and Accreditation of Systems

Certification and accreditation ensures that information systems' security controls are implemented correctly and operating as intended and that an agency official has authorized operation of the system based on those security controls.

Source: National Institute of Standards and Technology.

As of September 30, 2004, the FDIC had established a baseline level of assurance for its major applications and general support systems by performing certifications and accreditations at a low level of assurance. At that time, the FDIC recognized that some of its major applications and general support systems required a higher degree of security assurance in order to be considered fully certified and accredited in accordance with the National Institute of Standards and Technology (NIST) standards and guidelines. As of January 2005, the FDIC expected to fully certify and accredit all major applications and general support systems within 15 months in accordance with NIST standards and guidelines.

² A major application requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or modification of or unauthorized access to information in the application. A general support system is an interconnected set of information resources under the same direct management control and that shares common functionality. Such a system normally includes hardware, software, data, applications, communications, and people.

Other Corporate Efforts to Promote E-Government

The FDIC had made significant strides in using technology to promote safety and soundness in the banking industry, protect consumers' deposits, and quickly resolve bank failures. To reduce reporting burdens and to share information more quickly and conveniently, the FDIC had instituted several projects to promote E-Government. Synopses of various FDIC activities follow.

- **FDICconnect.** *FDICconnect* was designed for FDIC-insured institutions as an Internet channel to conduct business and exchange information with the FDIC. *FDICconnect* is designed to provide a secure e-business transaction channel to support implementation of the GPEA, which requires agencies to provide on-line consumer and business alternatives for paper-based processes when practicable. The FDIC plans to expand the number of *FDICconnect* applications, making it the standard electronic gateway for interactions with all insured institutions.
- **Virtual Supervisory Information on the Net (ViSION).** ViSION provides automated support for many aspects of bank supervision, including application tracking, case management, safety and soundness examinations, IT examinations, off-site monitoring, large bank analysis, management reporting, workload management, and security. ViSION allows FDIC examiners to operate more efficiently by working with electronic rather than paper-based information.
- **FDICSales.com.** The FDICSales Web site provides customers with the convenience of on-line access 24-hours a day to FDIC loan sales events. Customers can register their preferences for the types of loans they are interested in purchasing, receive electronic notification of sales matching their preferences, access detailed information concerning the loans offered for sale, and submit bids to purchase the loans. Through FDICSales.com, potential bidders can also review financial and other detailed information and submit bids on a failing bank or thrift and on loan pools not sold within a bank at the time of failure.
- **Call Report Modernization.** Reports of Condition and Income (Call Report) are a widely used source of timely and accurate financial data regarding a bank's condition and the results of operations. The Call Report Modernization effort is an interagency initiative that targets improvements in the compilation, collection, validation, integration, and distribution of financial and demographic data related to FDIC-insured institutions. The initial focus of the project has been on modernizing the process through which the FDIC and other federal regulators acquire Call Report data. The FDIC has taken a leadership position in the definition and implementation of the Call Report Modernization initiative, collaborating closely with the Board of Governors of the Federal Reserve System and the Office of the Comptroller of the Currency.
- **Corporate Human Resource Information System (CHRIS).** CHRIS includes a new Web-based, employee self-service time and attendance system based on a

commercial off-the-shelf system designed specifically for use with the National Finance Center payroll system. CHRIS will provide the FDIC with an integrated system that supports all existing human resources functions with a focus on data sharing, state-of-the-art computing technology, and the ability to grow and change with the Corporation's business needs.

Process and Plan for Implementing E-Government Initiatives

Agencies have established a process and plan for implementing all of the E-Government initiatives rather than creating redundant or agency-unique IT projects.

Source: *Expanded Electronic Government Scorecard Criteria.*

As discussed earlier, the FDIC had taken initiatives and developed systems that were in line with E-Government principles; however, these systems and initiatives were separate development efforts rather than the fulfillment of a comprehensive plan. In September 2002, the FDIC published the *FDIC E-Government Strategy*, which defined the FDIC's strategy for E-Government service delivery and presented the critical supporting factors required to implement E-Government initiatives. However, this document did not discuss goals and objectives or desired outcomes.

Key to managing any successful IT program is establishing IT goals and objectives, measuring performance, and evaluating and reporting results to senior management. Measuring performance against established goals and objectives is a fundamental principle of the Government Performance and Results Act (GPRA) of 1993. In addition, OMB Circular No. A-130, *Management of Federal Information Resources*, requires agencies to institute performance measures and management processes that monitor actual performance against expected results.

The FDIC submitted a status report to OMB documenting the FDIC's progress in achieving E-Government. Specifically, the FDIC's June 26, 2003 progress report to OMB stated that the Corporation had completed development of an E-Government strategic plan that defines the FDIC's broad E-Government vision and mission, the FDIC's objective in developing E-Government, and the foundations needed to establish E-Government and barriers to its acceptance and implementation. However, in December 2004, DIT officials noted that the strategic plan had not been updated since it was prepared in September 2002 and that this initial effort had been general in nature. Consistent with the DIT officials' views, we found that the 2002 strategic plan did not include specific goals for the FDIC's E-Government initiatives, the resources needed, strategies to be followed, assigned responsibilities, or

performance measures for tracking accomplishments. Further, the plan was not supported by or linked to corporate goals and objectives established under GPRA or the Corporate Performance Objectives (CPO).³

In August 2004, the FDIC issued the *Information Technology Strategic Plan: 2004–2007* (IT Strategic Plan). The IT Strategic Plan is one tool that the Corporation uses to set its strategic direction for IT. The purpose of the IT Strategic Plan is to align IT with the FDIC’s mission, vision, and business goals and to establish the overall goals and direction for the IT Program at the FDIC. The IT Strategic Plan describes how IT helps accomplish the FDIC’s mission. The IT Strategic Plan also outlines many of the projects and programs, such as ViSION and FDICSales.com, that support the E-Government initiative and considers IT support for “Expanded Electronic Government” as a means to operate more efficiently and effectively. Like the *FDIC E-Government Strategy*, the IT Strategic Plan does not specifically identify measures for implementing the expanding E-Government initiatives and does not contain goals, performance measures, objectives, and desired outcomes consistent with those initiatives.

During our review, the Corporation established a CPO in December 2004 to develop and implement a new E-Government strategy. The strategy will promote a paperless corporate environment in which the majority of transactions and data and document storage are handled electronically. The FDIC also established a working group that developed a scoping statement that was approved by the CIO Council and a draft project plan to guide development of the E-Government strategic plan. The scoping statement addresses performance measures related to only one initiative -- promoting a paperless environment. The project plan does not specifically address either performance measures or desired outcomes for the E-Government initiatives.

Conclusion

The FDIC had been actively identifying, evaluating, and implementing various policies, procedures, and technologies that are consistent with the goals and principles of the E-Government initiatives and implementing OMB guidance. However, the FDIC needed to better coordinate and measure its efforts through the timely development of a strategic plan that is linked to corporate objectives and goals specifically addressing E-Government. The plan, objectives, and goals would assist the Corporation in making steady progress in various aspects of E-Government, minimizing redundant systems or processes, and undertaking initiatives that are cost-beneficial.

At our exit conference, DIT officials indicated that the Corporation has established a milestone of December 31, 2005 for the CIO Council to approve a new E-Government strategic plan.

³ The FDIC initiated the CPOs in 2002, which set an overall direction for the Corporation and go beyond the operational goals established in the Corporation’s Annual Performance Plan sent to the Congress and OMB. The CPOs are established each year during the annual corporate planning and budget process, subject to final approval by the Chairman.

The actions taken by the Corporation during and subsequent to our review, together with its planned actions, adequately address our finding. Thus, we are not making any recommendations. We suggest, however, that in completing the new E-Government strategic plan, the Corporation be mindful of the August 2003 OMB E-Government Act guidance that E-Government performance measures must be linked to the Corporation's Annual Performance Plan and Strategic Plan and desired outcomes of E-Government must be identified.

CORPORATION COMMENTS AND OIG EVALUATION

We provided FDIC management with a draft of this report on April 14, 2005. The draft report included two recommendations associated with establishing an E-Government strategic plan. Subsequent to issuance of the draft report, we held an exit conference with management to discuss our findings and proposed recommendations. As discussed earlier in this report, management provided us with additional information regarding several actions it had taken during and after our review, as well as planned actions, that adequately addressed our concerns regarding the need for an E-Government strategic plan. As a result, we made appropriate changes to the final report, including eliminating the recommendations. We provided management with a revised version of the draft report reflecting those changes and a written response was not required. DIT notified the OIG that it had no official comments on the revised draft report.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our audit was to determine whether the FDIC (1) adequately implemented E-Government principles in its operations and information exchange with insured financial institutions and (2) complied with applicable portions of the GPEA. The audit was conducted from December 2004 through March 2005 in accordance with generally accepted government auditing standards. The scope of our audit work was limited to obtaining an understanding of the Corporation's progress on E-Government initiatives because the FDIC had not developed a comprehensive E-Government strategic plan. We used areas in OMB's Scorecard tracking system to assess the FDIC's progress in implementing E-Government.

Regarding GPEA, the FDIC has developed several applications and initiatives that have been designed to reduce paperwork or streamline processes internally and externally. Because we limited the scope of our audit, we did not determine whether these initiatives fully comply with the intent of the Act. However, we verified that the FDIC submitted its progress report to OMB, describing the Corporation's progress in complying with GPEA.

To accomplish our objective, we reviewed numerous documents including:

- Public Law 107-347, also referred to as the E-Government Act of 2002;
- OMB's *E-Government Strategy*, dated February 27, 2002;
- Public Law 105-277, Government Paperwork Elimination Act;
- OMB's *E-Government Strategy*, dated April 2003;
- OMB's *Implementation Guidance for the E-Government Act of 2002*, dated August 2003;
- OMB's *Expanding E-Government, Partnering for a Results-Oriented Government*, dated December 2004;
- OMB's Executive Branch Management Scorecard;
- Public Law 103-62, Government Performance and Results Act;
- OMB Circular No. A-130, *Management of Federal Information Resources*;
- the *FDIC E-Government Strategy*, dated September 2002;
- FDIC's *Information Technology Strategic Plan: 2004-2007*; and
- FDIC's CIO Council E-Government Strategy Project Plan Draft.

Applicability of Initiatives, Guidance, and Legislation to the FDIC

In conducting this audit we considered the PMA, portions of which were codified in the E-Government Act of 2002 enacted December 17, 2002. While the PMA may not be binding on the FDIC, many of the provisions of the E-Government Act are binding on the FDIC. Our review focused on title II of the Act, *Federal Management and Promotion of Electronic Government Services*, because of its applicability to this audit. Under the Act, OMB has authority to issue guidance to implement the Act's provisions, and such guidance is, in general, binding on the FDIC. Accordingly, OMB's August 2003 *Implementation Guidance*

APPENDIX I




for the E-Government Act of 2002 appears to be binding on the FDIC. OMB's February 2002 *E-Government Strategy* predates the E-Government Act and does not reference any other statutory or regulatory authorities for its issuance and thus is not legally binding on the FDIC. OMB's Scorecard has been used to track the progress of various departments and agencies, but has not included the FDIC.

While OMB's pronouncements discussed above may or may not be legally binding on the FDIC, we believe they represent prudent business practices that the FDIC should consider in its E-Government efforts. Accordingly, we employed those pronouncements, particularly the Scorecard analysis, in performing this audit.

GPRA, Reliance on Computer-Generated Data, Fraud and Illegal Acts, and Management Controls

We tested compliance with the GPRA by determining whether the FDIC had established performance measures related to E-Government initiatives. The limited nature of the audit did not require testing internal controls or reviewing the reliability of computer-processed data obtained from the FDIC's computerized systems. Such data was not significant to our audit findings and conclusions. During the audit, we were alert for instances of fraud and illegal acts, but found none.

EXPANDED ELECTRONIC GOVERNMENT

		
<p>Agency:</p> <ul style="list-style-type: none"> Has an Enterprise Architecture linked to the Federal Enterprise Architecture (FEA) rated “effective” using OMB’s EA Assessment tool (score of “3” on both EA Maturity and Degree of Alignment); Has acceptable business cases (security, measures of success linked to the Enterprise Architecture, program management, risk management, and cost, schedule, and performance goals) for all major systems investments; Has demonstrated using EVM or operational analysis, cost and schedule overruns, and performance shortfalls, that average less than 10% for all major IT projects; Submits quarterly status reports in remediating IT security weaknesses; Inspector General verifies the effectiveness of the Department-wide IT Security Remediation Process; Has 90% of all IT systems properly secured (certified and accredited); AND Has implemented all of the appropriate E-Gov initiatives rather than creating redundant or agency unique IT projects. <ul style="list-style-type: none"> To maintain green status, agency: Has ALL IT systems certified and accredited; Has IT systems installed and maintained in accordance with security configurations; AND Has consolidated and/or optimized all agency infrastructure to include providing for continuity of operations. 	<p>Agency:</p> <ul style="list-style-type: none"> Has an Enterprise Architecture linked to the FEA rated “effective by using OMB’s EA Assessment tool (score of “3” on both EA Maturity and Degree of Alignment); Has acceptable business cases (security, measures of success linked to the EA, program management, risk management, and cost, schedule and performance goals) for more than 50% of its major systems investments; Submits security reports to OMB that document consistent security improvement and either: <ul style="list-style-type: none"> 80% of all IT Systems are properly secured; OR Inspector General verifies the effectiveness of the Department-wide IT Security Plan of Action and Milestone Remediation Process; Has cost and schedule overruns, and performance shortfalls, that average less than 30% for all major IT projects; AND Has established a process and plan for implementing all of the appropriate E-Gov initiatives rather than creating redundant or agency unique IT projects 	<p>Agency:</p> <ul style="list-style-type: none"> Does not have an Enterprise Architecture linked to the FEA that “effective” by using OMB’s EA Assessment tool (score of “3”); Does not have acceptable business cases (security, measures of success linked to EA, program management, risk management, and cost, schedule and performance goals) for more than 50% of its major systems investments; Has not submitted Security Reports to OMB that document consistently security improvement and cannot demonstrate that: <ul style="list-style-type: none"> 80% of all IT systems are properly secured; OR Inspector General has verified the effectiveness of the Department-wide IT Security Plan of Action and Milestone Remediation Process; Has cost and schedule overruns, and performance shortfalls, that average 30% or more; OR Has not established a process and plan for implementing all of the appropriate E-Gov initiatives rather than creating redundant or agency unique IT projects.

Source: Reproduced from OMB.

Note: Earned Value Management (EVM) is operational analysis of cost overruns and performance shortfalls to average less than 10 percent of an IT portfolio.