

Office of Inspector General



May 24, 2001
Audit Report No. 01-011

Development of the FDIC's Public Key Infrastructure



DATE: May 24, 2001

TO: Donald C. Demitros, Director, Division of Information Resources Management,
and Chief Information Officer



FROM: David H. Loewenstein
Assistant Inspector General

SUBJECT: Audit of the *Development of the FDIC's Public Key Infrastructure* (Audit Report No. 01-011)

The Federal Deposit Insurance Corporation's (FDIC) Office of Inspector General (OIG) has been involved in auditing the development of the Corporation's public key infrastructure (PKI) since 1997. The objectives of this audit were to ensure that the development of the FDIC's PKI (1) follows a structured approach, (2) addresses user requirements, (3) considers viable alternatives, (4) is adequately tested, and (5) incorporates needed controls. In accomplishing our objectives, we determined if the FDIC's PKI will meet generally recognized security standards, be sanctioned by the U. S. General Accounting Office (GAO) for use with the FDIC's fully automated financial systems that affect the annual financial statements, and benefit from "lessons learned" at other federal agencies. This report discusses our interaction thus far with the Divisions of Information Resources Management (DIRM) and Finance (DOF), GAO, the National Institute of Standards and Technology (NIST), and interested parties from other federal agencies. Our report also provides recommendations regarding certain future steps DIRM and the corporate user community should take when developing and implementing the FDIC's PKI and the automated systems that will use digital signature technology.

BACKGROUND

In recent years, the dramatic rise in computer technology has changed the ways individuals, businesses, and government entities interact. Business-to-business transactions are increasingly being accomplished through the Internet and other means of electronic data exchange. Government agencies have implemented many E-government applications, including the purchase of goods and services, electronic claim filing, and client applications for federal benefits.

Recent legislation such as Public Law 105-277, the *Government Paperwork Elimination Act* (GPEA), enacted on October 21, 1998, and Public Law 106-229, the *Electronic Signatures in Global and National Commerce Act* (ESIGN), enacted on June 30, 2000, will accelerate the

implementation of e-commerce activities throughout the federal government. Specifically, GPEA requires federal agencies to allow individuals and entities the option of submitting information or transacting with agencies electronically, whenever feasible. GPEA sets October 2003 as the deadline for federal agencies to provide individuals and entities that deal with them the option of electronic maintenance, submission, or disclosure of data as a substitute for paper. GPEA also assigns the Office of Management and Budget (OMB) the responsibility for ensuring that federal agencies meet the October 2003 deadline. To promote a structured process for complying with GPEA, OMB has issued implementation guidance that describes the process and principles that agencies should employ when evaluating, using, and accepting electronic signatures. OMB also required federal agencies to submit a GPEA implementation plan and schedule by October 2000. In addition, ESIGN has established the legal validity of electronic signatures throughout the United States and applies to any transactions that affect interstate or foreign commerce.

A recent GAO report, *ELECTRONIC GOVERNMENT: Government Paperwork Elimination Act Presents Challenges for Agencies*, dated September 2000 identified the challenges that lie ahead as federal agencies adopt e-commerce activities to transition to E-government. These challenges include sound IT investment policy, adequate and documented systems architecture, effective security and privacy, PKI interoperability,¹ reliable record keeping, and the provision for expertise and training.

To provide adequate controls and security for systems using electronic signatures, an application needs to validate the identity of the individual approving the documents and ensure that the data associated with the approval cannot be modified without detection. PKI is the methodology that has been developed to provide electronic signature technology in an effective and efficient manner. NIST has taken a leadership role in the development of standards for federal PKIs that will support electronic signatures and other security services.

The FDIC initiated the development of the Corporation's PKI in late 1996. In 1997, the OIG issued a memorandum to the Director of DIRM and another to the Directors of DIRM and DOF. The memoranda suggested that the FDIC (1) adopt electronic signature software, hardware, and techniques that comply with NIST guidelines; (2) issue a directive stating that the selected electronic signature software, hardware, and techniques will apply to all FDIC systems using that technology; (3) contact other federal agencies that have received GAO's sanction of their electronic signature modules to determine whether the FDIC could make use of other agencies' development efforts; and (4) develop a fully documented long-range plan to bring the FDIC's electronic signature module into agreement with federal PKI functionality. The FDIC had implemented all of our suggestions as of January 2001.

On June 30, 1998, our office issued an audit report entitled *Audit of Implementation of Electronic Signatures to Support the Electronic Travel Voucher Payment System (ETVPS) and Other Planned Systems* (Audit Report Number 98-052). In that report, we determined that the FDIC was proposing to use an electronic signature module that may not have provided adequate security for corporate-wide use. We also found that a lack of coordination within DIRM

¹ PKI interoperability is the ability of differing public key infrastructures to exchange electronically signed documents. The federal government is developing a "bridge" certificate authority (CA) to accomplish this. The FDIC will use a bridge CA to cross-certify with other entities.

precluded other system development efforts requiring electronic signature technology from being included in corporate requirements. In the report we recommended that the Director, DIRM (1) establish a long-range PKI development plan, (2) perform an alternatives analysis comparing the available alternative for providing FDIC's electronic signature needs, and (3) ensure that DIRM security personnel and system development project managers communicate on a regular basis to identify requirements for electronic signatures. All recommendations had been implemented by DIRM as of January 2001.

Since issuing the memoranda and report, the OIG has continued to work closely with DIRM, NIST, and GAO personnel by reviewing the development of the FDIC's PKI. DIRM established a PKI project plan that included additional tasks and milestones for bringing the electronic signature component of its PKI into compliance with NIST standards for high-risk systems. DIRM also initiated working groups with (1) NIST and GAO to develop a compliant PKI, (2) federal agencies involved in the federal PKI project, and (3) other federal financial institution regulatory agencies to share best practices for PKI development. In addition, DIRM began developing needed PKI documentation, such as the certificate policies and practices statement² that GAO deemed necessary to follow a structured PKI development process. Additionally, DIRM developed a certificate policy statement for a single PKI with four levels of assurance, basic, low, medium and high, as GAO had recommended. We estimate that the FDIC expended more than \$3 million through calendar year 2000 to develop and maintain its PKI.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to ensure that the development of the FDIC's PKI (1) follows a structured approach, (2) addresses user requirements, (3) considers viable alternatives, (4) is adequately tested, and (5) incorporates needed controls. This interim phase of our audit applied these objectives to the planning and development of the PKI by the FDIC with the assistance of GAO and NIST.

To address these objectives, we reviewed PKI documentation developed by DIRM for compliance with NIST and GAO standards and other generally accepted PKI practices. In addition, we interviewed and held status meetings with DIRM, NIST, and GAO personnel involved in the PKI development process. Finally we tracked the ability of DIRM to meet agreed upon milestone dates. The audit was performed between February 2000 and January 2001 in accordance with generally accepted government auditing standards. Due to the evolving nature of the PKI development process, we will continue our audit involvement throughout the process.

RESULTS OF AUDIT

Between 1997 and mid-2000, the FDIC developed and implemented a low assurance PKI that was used for the Electronic Travel Voucher Payment System (ETVPS). However, less significant progress was made in developing a single PKI for all levels of assurance. While the

² Certificate policies and practices are the documents that initially describe the concept of operations that the FDIC will use to develop its PKI.

FDIC's progress developing its PKI indicates that it is pursuing an effective course of action in addressing the tasks needed to implement an effective PKI that will benefit the Corporation and meet GAO sanctioning requirements, additional actions described in this report can further enhance the FDIC's efforts. Specifically, DIRM PKI personnel should ensure that all PKI-related documents are developed using NIST standards and GAO guidelines, and adhere to newly established PKI development milestones. In addition, using OMB's GPEA guidelines, the Director, DIRM, and Chief Information Officer (CIO) should develop an E-Government implementation plan.

THE FDIC HAS MADE PROGRESS IN PKI DEVELOPMENT BUT MORE REMAINS TO BE DONE

Since 1997, we have provided DIRM with our suggestions and recommendations for improving its PKI development process. After a slow start in developing a single PKI that encompassed all four levels of assurance - basic, low, medium and high, DIRM began substantive discussions in 2000 with NIST and GAO regarding the development of a compliant PKI. Our office has continued to maintain an active presence in the development of the FDIC's PKI by reviewing required PKI documentation and attending PKI status meetings with DIRM, DOF, GAO, NIST, and personnel from other federal organizations. DIRM's actions to date to develop an effective and compliant PKI have resulted in significant progress. We believe that the additional actions described in this report can further improve the process and enhance assurance of effective coordination between all involved parties.

PKI Development Process Can Be Expedited

In the early stages of development, the FDIC did not progress as quickly as anticipated in developing a secure PKI. For example, the original DIRM PKI development plan, developed in response to our June 30, 1998 audit report contained critical tasks and milestones for the development of the PKI. The critical elements of the plan included the development of a PKI concept of operations that complied with NIST standards for high-risk systems by August 1998 and the delivery of NIST-compliant PKI hardware for high-risk users by June 1999. Neither task had been attained as of December 31, 2000. However, during 2000 DIRM re-focused its efforts and made progress completing the tasks.

During 2000, we were actively involved in reviews of a memorandum of understanding (MOU) between DIRM and NIST, and the FDIC's PKI certificate policies and practices. The MOU between the FDIC and NIST described the roles and responsibilities of each organization, deliverables, and funding for the development of the FDIC's PKI. The MOU was completed in August 2000, and the certificate policies and practices were in the draft stage as of January 31, 2001. Further, DIRM personnel have begun using instructions and examples provided by GAO for the development of PKI deliverables.

On September 22, 2000, we met with DIRM, DOF, and GAO personnel involved in the FDIC's PKI development process. At that meeting, we determined that DIRM's progress in implementing a high-risk level PKI was still behind the original schedule. DIRM management

expressed concerns about the labor-intensive process needed to ensure adequate controls during the PKI certificate issuance process. The need for effective controls during this process is critical to implementing a PKI for high-risk transactions because of the increased need to ensure the identity of the individual being assigned the certificate. A GAO representative involved in the sanctioning process described a number of alternatives for handling the initial registration and certificate re-issuance processes and offered to provide DIRM management with points of contact at other federal agencies that had used effective methods. DIRM personnel agreed to consider these processes. The GAO representative also stated that a certificate policy statement was needed with practice statements for each of the four different levels of assurance required of an effective PKI. These levels provide for basic assurance, low assurance, moderate assurance, and high assurance.

During the meeting, DIRM agreed to expedite its PKI activities, develop and implement an effectively controlled certificate issuance process, and develop a high-level policy for its PKI. Since that meeting, DIRM has enhanced its efforts to develop a PKI that meets GAO and NIST guidelines and has developed a new PKI project plan. The plan includes such critical FDIC activities as the completion of the certificate policy and practice statements by October 2001, and an application program interface (API) functional review by January 2002. The function review is performed to ensure that the API contains all the functionality needed to properly interface with all applications that will use the PKI. If adhered to, the schedule will permit NIST to fulfill its role and test the API by the scheduled February 2003 goal. Other tasks that are scheduled to be completed by February 2003 include software and hardware upgrades to the digital signature module and required documentation. These documents include a concept of operations, audit procedures, certificate practices statements for all assurance levels, API usage guidelines, architecture description, disaster recovery procedures; and operating instructions for the certificate and registration authorities.

Recommendations

The Director, DIRM, and CIO should continue to ensure that:

- (1) all documents required for a NIST-compliant PKI are developed using NIST standards and GAO guidelines.
- (2) PKI development personnel adhere to the established milestones for the development and implementation of the FDIC's PKI.

Better Planning and Coordination Between DIRM and Future PKI Users Would Facilitate the FDIC's Transition to E-Government

Over the past 3 years, the FDIC initiated development of several fully automated systems that were intended to reduce costs and paperwork. Only one of these systems, ETVPS, has been placed into production. Many of the planned systems were being designed to provide for electronic approval of documents for payment or other authorization purposes. However, FDIC

management has yet to develop a business case that justifies the use of electronic signatures as a needed security measure for a planned or existing application.

In a June 30, 1998 audit report, we reported that an increase in internal coordination within DIRM was needed to ensure that all system requirements for the use of electronic signatures were addressed. We recommended that the Director, DIRM, ensure that security personnel and project managers communicate on a regular basis to identify future requirements for electronic signatures and other security needs.

Our office attended meetings with GAO, DOF, and DIRM personnel on November 8, 2000 and December 7, 2000. At those meetings, we determined that increased communication between DIRM and its clients regarding the roles and responsibilities of each office in the development of the FDIC's PKI would expedite the development of an overall strategic plan to implement PKI as part of the FDIC's transition to E-government. We also determined that an existing or planned candidate application that could effectively employ the FDIC's PKI had not been designated. A GAO representative stated that client organizations, with DIRM's assistance, should designate a candidate application, existing or planned, to initially employ the FDIC's PKI.

Active communication between DIRM and its clients in identifying and preparing business cases for existing and new applications that should employ PKI can help to ensure timely implementation of an effective E-government plan. This plan should address the challenges GAO identified in its report, *ELECTRONIC GOVERNMENT: Government Paperwork Elimination Act Presents Challenges for Agencies*. These challenges include the impact that E-government will have on the Corporation's IT investment policy, system architecture, security and privacy, PKI interoperability, record keeping, and needed expertise and training. This plan should also evaluate all existing and planned applications and develop a business case for each application as to what method of security, including the use electronic signature technology, is required for the transition to E-government. After the evaluation of all applications, the plan should identify the initial application that will avail itself of the new PKI technology. Finally, the plan should require that security personnel are involved in the earliest stages of application planning for the transition to E-government.

With the passage of GPEA and ESIGN, the transition to E-government has been accelerated. PKI has emerged as one of the most important security solutions to e-business. As organizations increase the level of security sophistication, different organizations must coordinate the development of their PKIs. Without this coordination, PKIs may be developed without the ability to inter-operate.

We believe the thrust of GPEA is to accelerate the transition to E-government by requiring federal agencies to develop a business case for using electronic signatures in all transactions with third parties. The ESIGN legislation complements GPEA in that it gives legal validity and enforceability within the United States to the use of electronic records and signatures in interstate and foreign commerce. We also believe that the FDIC could enhance its ability to ensure a seamless transition to E-government by closely adhering to OMB's GPEA guidelines in planning the transition. In this way, the FDIC would follow the same process and timelines as other federal agencies, thus ensuring that PKI security and interoperability problems are minimized.

It is imperative that coordination between DIRM's security and development personnel and the FDIC's user community begin at the earliest stages of the system planning process. Without the early involvement of security personnel in such a technical area as PKI, the project developers may need to re-formulate system plans to ensure that the technicalities of PKI and electronic security issues are adequately addressed. We also believe that before a high-risk candidate application is selected for use in PKI testing, a business case should be developed for all critical FDIC applications to determine which applications will require electronic signatures. Without this approach, the FDIC may have problems coordinating the development of the PKI and in its transition to E-government.

Recommendation

The Director, DIRM, and CIO should (3) develop an E-government implementation plan that uses OMB's guidelines for the implementation of GPEA and addresses the challenges outlined in GAO's report on electronic government.

CORPORATION COMMENTS AND OIG EVALUATION

On March 19, 2001, the CIO provided a written response to the draft report. The CIO generally agreed with the report's findings and recommendations and provided the elements necessary for management decisions on all three of the recommendations. The CIO's response is presented in its entirety in Appendix I of this report.

With regard to recommendations 1 and 2, the CIO indicated that DIRM will continue to enhance its efforts to develop a fully documented PKI and work closely with the OIG to complete the PKI development.

In his response to recommendation 3, the CIO noted that our report links PKI with the implementation of GPEA and stated that GPEA does not mandate the use of PKI but describes a spectrum of currently available electronic signature technologies. We agree with the CIO's interpretation of GPEA and understand that all applications may not require the use of a PKI. However, for clarification, it should be noted that most of the electronic signature technologies that the CIO described are identified in OMB's guidance as non-cryptographic³ methods of authenticating identity. That is, the CIO is referring to such methods as personal identification numbers, smart cards, digitized signatures and biometrics. We believe that if one reads OMB's explanation of electronic signature technologies in its entirety, it is clear that the digital signature methodology as implemented through PKI (a cryptographic method) is the only technology that binds the identity of the signatory to the contents of a document. It is for this reason that we have discussed PKI as the optimum method of implementing both electronic signature and other security features. We have done so because PKI is a robust method of providing an electronic signature and is the only current method that provides for non-repudiation of electronic

³ Cryptography is the art or process of writing or deciphering secret code. Effective use of cryptography provides the ability to securely exchange information with selected recipients.

signatures. This ability coupled with the fact that the FDIC has expended over \$3 million developing a PKI model that currently interfaces with the ETVPS strongly suggests to us that PKI provides a cost-effective solution to the FDIC's electronic signature needs. Ultimately, the determination of when to utilize PKI technology must be made based on the business case and assessed risk associated with the application. The CIO has stated that DIRM is committed to the development of an e-business plan that meets the intent of GPEA. We believe that if DIRM meets all of the stated objectives and goals of that plan, PKI will be identified as a major part of the FDIC's evolution to E-government.

APPENDIX I
CORPORATION COMMENTS




Federal Deposit Insurance Corporation
3501 North Fairfax Dr. Arlington, VA 22226

Office of the Chief Information Officer

March 19, 2001

TO: David H. Loewenstein
Assistant Inspector General

FROM: Donald C. Demitros
Chief Information Officer 

SUBJECT: DIRM Management Response to the Draft OIG Report Entitled, "Development of the FDIC's Public Key Infrastructure" (Audit Number 2000-90.)

The Division of Information Resources Management (DIRM) has reviewed the subject draft audit report and generally agrees with the findings and recommendations. As a general comment, it appears that the report links Public Key Infrastructure (PKI) closely with the implementation of the Government Paperwork Elimination Act (GPEA). We would like to note that GPEA does not mandate that one particular form of electronic signature be used for E-government. The "OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act" describes a spectrum of currently available electronic signature technologies, such as: PIN or password, smart card, digitized signature, biometrics, shared symmetric key cryptography, and public/private key cryptography (digital signatures). As the FDIC moves forward with our E-government activities, we will take advantage of the most appropriate technologies to meet our business requirements.

The management decision for each specific recommendation is provided below.

Recommendations: The DIRM Director, and CIO should continue to ensure that:

- (1) All documents required for a NIST-compliant PKI are developed using NIST standards and GAO guidelines.

DIRM Response: DIRM agrees with the OIG recommendation and will continue to enhance its efforts to develop a fully documented PKI that meets GAO and NIST guidelines. All documentation supporting this effort will be developed using NIST standards and GAO guidelines. DIRM will also continue to ensure the involvement of the OIG in the review and comment of the PKI program and technical documentation.

- (2) PKI development personnel adhere to the established milestones for completing the development and implementing the FDIC's PKI.

DIRM Response: DIRM agrees with the recommendation and will continue to work closely with the OIG to complete the development and implementation of the FDIC's PKI and

ultimately GAO PKI sanctioning. The Information Security Staff updated its PKI project plan in February, 2001 and established new milestones for completing the Entrust update of Version 4 on the network servers, review of the certificate policy and development of a PKI application program interface. To ensure the best possible adherence to the current project milestones, the Deputy Director, Information Technology Management has established a biweekly status meeting with the DIRM PKI project team. The status of all outstanding PKI related milestones will be reviewed at each meeting beginning in March 2001.

Recommendation: The DIRM Director, and CIO should:

- (3) Coordinate with other FDIC divisions and offices to develop an E-government implementation plan that uses OMB's guidelines on the implementation of GPEA. The plan should (a) determine the impact that E-government will have on the Corporation's IT investment policy, system architecture, security and privacy, record keeping, and needed expertise and training; (b) evaluate all existing and planned applications and develop a business case for each application as to what method of security, including the use electronic signature technology is required for the transition to E-government; and (c) identify the initial application that will avail itself of the new PKI technology, and (d) ensure that security personnel are involved in the earliest stages of application planning for the transition to E- government.

DIRM Response:

The FDIC is initially addressing many aspects of E-government implementation as part of the FDICconnect initiative. DIRM has issued a Request For Proposals for a contract to develop an e-business strategy and plan. Responses for this RFP are due 3/23/2001. The e-business plan that will result from this contract will address many of the components identified in this recommendation. We currently anticipate that the draft strategy and plan will be completed by 6/30/2001 and the final version completed by 12/31/2001. Specifically,

- a) Corporate IT Investment Policy - There is an objective to establish a plan for developing requirements for transforming business processes and developing business cases to exploit e-business opportunities. The project will also develop e-business goals and objectives and ensure that they can be integrated with corporate strategic goals which drive DIRM's IT investment policy. The contract will include the analysis of alternatives for the e-business technical architecture including a cost-benefit analysis.

System Architecture - The contract calls for the definition and refinement of the e-business technological and security architecture emphasizing integration into FDIC's system architecture. The effort will require the analysis of any gaps between the current

technical architecture and the FDIC e-business vision and require the development of strategic actions to achieve the FDIC target technical environment.

Security and Privacy - In support of the E-Business Technical Architecture Team, the contract will include an analysis of the current e-business security architecture and the development of recommendations for the target e-business architecture including security. The contract calls for ensuring that e-business initiatives are consistent with the Security Policy Memo 98-012, "FDIC Encryption/Digital Signature and Public Key Infrastructure Standard".

Record Keeping - As part of the e-business strategy, the contract calls for ensuring that e-business initiatives are consistent with the Government Paperwork Elimination Act and the Electronic Signature Act.

Needed Expertise and Training - While specific education and training activities will be addressed in subsequent contract initiatives, this contract will evaluate marketing and awareness activities related to the current *FDICconnect* project and identify lessons learned and best practices for future e-business implementations.

- b) The development of the corporate e-business strategy will address the necessary OMB guidelines on the implementation of GPEA. As part of the development of this strategy, one of DIRM's goals is to develop an architectural approach that addresses security issues, including electronic signatures. This strategy may be customer focused - for example, all transactions associated with institutions will use the *FDICconnect* platform. Once established, such a strategy will lead to the development of business cases and the evaluation of applications. As noted earlier, GPEA does not mandate that one particular form of electronic signature be used for E-government. There is a spectrum of currently available electronic signature technologies, such as: PIN or password, smart card, digitized signature, biometrics, shared symmetric key cryptography, and public/private key cryptography (digital signatures) that are legitimate solutions in the proper context. As the FDIC moves forward with our E-government activities, we will take advantage of the most appropriate technologies to meet our business requirements. Currently with *FDICconnect*, DIRM is working with Legal to determine the appropriate level of electronic signature required on a transaction by transaction basis. For example, for the first transaction that DIRM obtained legal consultation, Legal opined that the user id/password combination and the security model provided by *FDICconnect* were adequate in constituting a valid electronic signature for the DOF Assessment Payment Options form.
- c) Once completed, the e-business plan will include the identification of the initial application that will utilize PKI technology.

d) DIRM will ensure that security personnel are involved in the earliest stages of application planning for the FDIC's transition to E-government. For example, under the FDICconnect initiative, a security plan is being established as part of the pilot effort. The FDICconnect team has worked with the Information Security Staff (ISS) as follows:

- Copy of the functional requirements document for FDICconnect general security system reviewed by ISS;
- Primary Point-Of-Contact appointed from security;
- ISS participated in the review of and recommendation of the technical architecture for the FDICconnect pilot;
- Worked with ISS on how the FDICconnect servers would be connected to FDIC network;
- Consulted with ISS on firewall issues. Continue to work with ISS on a solution for data transfer through the firewall;
- Consulted with ISS on "timing delay" issues between IIS and NT;
- ISS participated in the issuance of server certificates for FDICconnect;
- FDICconnect team members attended a demonstration from ISS on the certificate process. The team continues to discuss client certificates and the potential for their use in FDICconnect;
- ISS performed a "sweep" of the FDICconnect servers for technical infrastructure.
- Working with ISS to develop sensitivity assessment questionnaires for each individual transaction; and
- ISS will participate in FDICconnect testing.

Please address any questions to DIRM's Audit Liaison, Rack Campbell, on (703) 516-1422.

MANAGEMENT RESPONSES TO RECOMMENDATIONS

The Inspector General Act of 1978, as amended, requires the OIG to report the status of management decisions on its recommendations in its semiannual reports to the Congress. To consider FDIC’s responses as management decisions in accordance with the act and related guidance, several conditions are necessary. First, the response must describe for each recommendation

- the specific corrective actions already taken, if applicable;
- corrective actions to be taken together with the expected completion dates for their implementation; and
- documentation that will confirm completion of corrective actions.

If any recommendation identifies specific monetary benefits, FDIC management must state the amount agreed or disagreed with and the reasons for any disagreement. In the case of questioned costs, the amount FDIC plans to disallow must be included in management’s response.

If management does not agree that a recommendation should be implemented, it must describe why the recommendation is not considered valid. Second, the OIG must determine that management’s descriptions of (1) the course of action already taken or proposed and (2) the documentation confirming completion of corrective actions are responsive to its recommendations.

This table presents the management responses that have been made on recommendations in our report and the status of management decisions. The information for management decisions is based on management’s written response to our report.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
1	DIRM will continue to ensure that all PKI documents follow NIST standards and GAO guidelines.	March 19, 2001	Management's response to the audit report.	N/A	Yes
2	DIRM will continue to ensure that PKI development personnel adhere to established milestones for completing PKI development.	March 19, 2001	Management's response to the audit report.	N/A	Yes
3	DIRM will coordinate with other FDIC divisions and offices to develop an E-government implementation plan.	December 31, 2001	E-business plan that contains the objectives and goals as described in management's response to the audit report.	N/A	Yes