GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

April 20, 2004

The Honorable Sue W. Kelly
Chairwoman
Subcommittee on Oversight and Investigations
Committee on Financial Services
House of Representatives

Subject: *Posthearing Questions Related to the Federal Deposit Insurance Corporation's 2003 and 2002 Financial Audits*

Dear Madam Chairwoman:

On March 4, 2004, I testified before your subcommittee at a hearing on oversight of the Federal Deposit Insurance Corporation (FDIC)[1] and discussed the results of our 2003 and 2002 audits of FDIC's financial statements.[2] This letter responds to subsequent questions that you asked me to answer for the record. The questions and my responses follow.

1. **The FDIC has made significant progress in correcting the computer security weaknesses identified in GAO's 2002 report. Do you feel that the FDIC is on the right path to correct the 22 new information security weaknesses identified through your oversight in 2003? How will GAO monitor the agency in the coming months to ensure that these weaknesses are addressed?**

FDIC has been responsive to addressing information security weaknesses we have previously reported. For example, during the past year, FDIC corrected 28 of 29 weaknesses that were still open from our 2002 calendar year financial audit. Similarly, prior to the completion of our audit, the corporation developed a comprehensive corrective action plan to address each of the 22 new information security weaknesses identified in our calendar year 2003 financial audit. If fully

[1]U.S. General Accounting Office, *Federal Deposit Insurance Corporation: Results of 2003 and 2002 Financial Audits*, GAO-04-522T (Washington, D.C.: Mar. 4, 2004).
[2] U.S. General Accounting Office, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2003 and 2002 Financial Statements*, GAO-04-429 (Washington, D.C.: Feb. 13, 2004).

and effectively implemented, FDIC's corrective actions should address each of the security deficiencies identified.

In addition to these 22 weaknesses, as we included in our testimony, a key reason for FDIC's continuing weaknesses in information system security controls is that it has not yet fully implemented all elements of a comprehensive security management program. Such a program is critical to resolving existing computer security problems and continuously managing information security risks, and includes a testing and evaluation program to ensure that systems are in compliance with policies and procedures and to identify and correct weaknesses that may occur. While FDIC has done much to establish a complete security management program, its review, testing, and evaluation program does not yet address all key areas. FDIC management currently has a plan in place to establish a comprehensive security management program that includes a complete review, testing, and evaluation program. Implementing such a program should allow FDIC to better identify and correct security problems, such as those identified in our 2003 audit.

We will continue to monitor FDIC's progress in addressing the 22 information security weaknesses and in implementing its comprehensive security management program. During the course of the next several months, we plan to meet periodically with FDIC's Chief Information Officer and his staff to discuss their progress in implementing their corrective action plans. Further, in connection with our calendar year 2004 financial audit, we will follow-up on the status of these weaknesses and perform tests, as appropriate, to determine whether adequate actions were taken to remediate the information security weaknesses.

2. In your testimony, you state that since the banking and financial services environment is constantly changing, the FDIC must continually monitor its business environment and related risks, and adapt its internal operations as well as its monitoring functions to manage risk and maximize its overall mission. What steps is GAO taking to uphold its high audit standards in this constantly changing financial services environment?

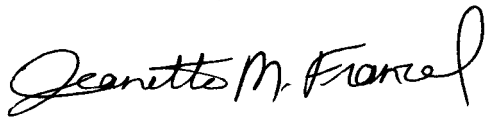
GAO has a two-pronged approach for keeping pace with the constantly changing environment in which we conduct our audits. First, we update our own audit methodology, the *Financial Audit Manual* (FAM), to reflect current issues and updated auditing standards. For example, soon we will be requesting comments on an exposure draft that will update the FAM, primarily to incorporate the provisions of Statement on Auditing Standards 99, *Consideration of Fraud in a Financial Statement Audit.* Second, during the audit process we monitor and review FDIC's actions to adapt and improve its operations to a changing environment. FDIC is currently in the process of changing the methodology it uses

to estimate potential failure and loss rates of insured financial institutions and of developing new financial systems to enhance its ability to meet financial management and information needs. As part of our audit, we will analyze FDIC's new and revised methodologies and programs to determine if they follow a reasonable approach and include the proper internal controls over the accuracy and completeness of the data being captured and the results.

We are sending copies of this letter to the Ranking Minority Member and Vice Chairman of your subcommittee. This letter is also available on GAO's Web site at www.gao.gov.

If you or your staff have questions about the responses to your questions, please contact me at (202) 512-9471 for financial issues or Robert Dacey at (202) 512-3317 for information technology issues. We can also be reached by e-mail at franzelj@gao.gov or daceyr@gao.gov.

Sincerely yours,



Jeanette M. Franzel
Director
Financial Management and Assurance

(194393)