Office of Inspector General

October 11, 2000
Evaluation Report No. 00-006

FDIC's Information Handling Practices for Sensitive Employee Data

Office of Congressional Relations and Evaluations

Federal Deposit Insurance Corporation
801 17th Street NW Washington DC 20434

Congressional Relations and Evaluations
Office of Inspector General

DATE: October 11, 2000

TO: Arleas Upton Kea
Director
Division of Administration

FROM: Stephen M. Beard
Assistant Inspector General

SUBJECT: *FDIC's Information Handling Practices for Sensitive Employee Data* (EVAL-00-006)

The Office of Inspector General's (OIG) Office of Congressional Relations and Evaluations (OCRE) has completed a review evaluating how the Corporation safeguards or protects sensitive employee data and records. This was the second in a series of reviews we plan to do on privacy-related issues.[1] Although we worked with other divisions and offices, this report was addressed to you because we believed the Division of Administration (DOA) could most effectively address our recommendations.

As you are aware, the need to protect personally identifiable information has never been greater. For purposes of this review, we defined sensitive employee data to be personally identifiable information including an employee's name, address, Social Security number (SSN), or medical information. This definition was consistent with reports and articles written about privacy. There was particular concern about the availability of SSNs because they often are the best gateway to obtain other personal information. The objectives of this review were to identify:

- various administrative documents and systems that include sensitive employee data and the controls designed to protect that information, and
- relevant policies and practices for handling sensitive employee data.

The intent of our work was to identify specific issues related to protecting the confidentiality of employee data that warrant management's attention or further review.

We found that the Corporation had policies and procedures designed to keep sensitive employee data confidential. Despite these measures, employee data was potentially vulnerable to the extent that employees did not follow procedures and general information system controls were

[1] In May 2000, OCRE issued a report entitled *FDIC's Privacy and Security Notices – Requirements and Policy Statements on the Internet and Intranet* (EVAL-00-004).

not fully implemented or operating as intended.[2] For example, we were told and observed that the Corporate Time and Attendance Worksheet (CTAW) was not always kept secure throughout the time and attendance process. Each CTAW contained an employee's name and SSN. With these two pieces of information, an identity thief could do damage. Specifically, SSNs were considered the key to large amounts of personal information, including tax information, credit information, school records, and medical records.

With respect to information systems containing employee data, officials described to us controls designed to limit access to and the authority to modify data in systems that include sensitive employee data. However, the U.S. General Accounting Office (GAO) identified weaknesses in FDIC's information systems general controls and included this as a reportable condition in its 1999 financial statement audit report.[3] GAO stated that until the Corporation fully implements its information security program, it might be difficult to ensure that its information system controls are operating as intended. In response to GAO's report, the Corporation stated that it will continue information system improvement efforts initiated in 1999 and will take additional corrective actions to address the issues and recommendations reported by GAO. The scope of our work in this area was limited. Accordingly, we made no conclusions or recommendations with respect to information systems.

We recommended that DOA periodically remind all employees about the need to routinely take precautions to keep sensitive employee data confidential. In addition, specifically related to CTAW, we recommended that DOA reevaluate our suggestion to mask or partially mask the employee's SSN on CTAW as an interim measure until CTAW is replaced. We believed it was important for DOA to reevaluate our suggestion if time and attendance software being considered during our review proved not to be viable option or was not implemented for an extended period of time.

Why is it important to keep sensitive employee data confidential?

The unnecessary disclosure of an individual's SSN creates the risk of confidential information being disclosed to any person or institution in possession of the individual's SSN.

Electronic Privacy Information Center Document

There has been increased concern over how personally identifiable data has been collected, used, and shared in both the government and private sectors. In general, privacy concerns have been defined to include the acquisition, use, and disclosure of personal information. Personal information that is ineffectively safeguarded could result in such information being used improperly, unfairly, or for purposes other than those intended by an individual. More specifically, identity theft occurs when someone obtains personal information about an individual without their knowledge to commit fraud or theft.

[2] Information system general controls include corporate-wide security program planning and management, access controls, system software, application software development and change controls, segregation of duties, and service continuity controls.

[3] *Financial Audit: Federal Deposit Insurance Corporation's 1999 and 1998 Financial Statements* (GAO/AIMD-00-157), GAO report dated May 2000.

Congress enacted the *Identity Theft and Assumption Deterrence Act of 1998* to provide citizens some recourse in resolving instances where their SSN has been misused. The Act sets forth criminal penalties for any person who knowingly transfers or uses, without lawful authority, the means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law or constitutes a felony under any state or local law. The phrase "means of identification" is defined to include any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual. The definition includes the following examples, among others, name, SSN, and date of birth.

In August 1999, the Social Security Administration OIG reported the expanded use of the SSN as a national identifier has given rise to individuals using counterfeit SSNs and SSNs belonging to others for illegal purposes.[4] More specifically, the Social Security Administration OIG reported that a large portion (35 percent) of all allegations made to its hotline were related to SSN misuse. Of the SSN misuse allegations it reviewed, 81.5 percent related to identity theft. Identity theft victims have had their credit histories destroyed by individuals who steal and use their SSN to obtain credit. Moreover, these victims have found that resolving credit problems resulting from identity theft can be time-consuming and frustrating. In fact, GAO has reported that the "human" costs of identity fraud can be very high.[5] These costs included emotional costs, as well as, various financial or opportunity costs. For example, victims might have been unable to obtain a job, purchase a car, or qualify for a mortgage.

To deter identity theft, individuals have been advised by experts to not unnecessarily disclose their SSN, not because disclosure in itself would be harmful, but because that information could be used to gain access to other information such as individual banking records or credit card numbers. For example, information brokers amass vast amounts of personal information, including SSNs, about members of the public for resale. When possible, information brokers retrieve data by SSN because it is more likely to produce records more unique to the individual than other identifiers. Furthermore, published reports and articles indicated that one illicit source of data in many cases was the workplace.

Indeed, privacy advocates have warned that privacy issues should not be ignored in the workplace. Accordingly, these advocates stated that organizations need to be extremely cautious about collecting, using, and disclosing SSNs of customers and employees. If lists of employee names and SSN were available within an organization, employees could be bribed or corrupted to sell them or can misuse the information themselves. Because this information is often sensitive, it should be kept confidential. At FDIC, there have been reported incidents where FDIC employees have intentionally misused information entrusted to them. In fact, the OIG's Office of Investigations was reviewing one such case during our review. Consequently, as an employer, FDIC needs to remain ever vigilant to minimize such opportunities for a dishonest employee.

In 1996, an internal task force studied how FDIC monitored, managed, and controlled sensitive documentary information throughout the Corporation. This confidentiality task force focused its

[4] *Analysis of Social Security Number Misuse Allegations Made to the Social Security Administration's Fraud Hotline* (A-15-99-92019), Social Security Administration OIG report dated August 1999.
[5] *Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited* (GAO/GGD-98-100BR), GAO report dated May 1998.

review on sensitive business documents. The task force concluded at that time that FDIC did not have a widespread problem with breaches of confidentiality. The task force further concluded that the efforts to promote a confidentiality culture should be reinforced and reemphasized over time at the corporate level.

What did our work involve?

Our review objectives were to identify:

- various administrative documents and systems that include sensitive employee data and the controls designed to protect that information, and
- relevant policies and practices for handling sensitive employee information.

As we stated above, for the purpose of this review, we defined "sensitive employee data" to include an employee's name, SSN, address, and health information. The scope of our review was broadly defined to include those divisions and offices in headquarters that we determined would routinely handle sensitive employee records or data. We primarily focused on offices within DOA. Specifically, we interviewed officials in the Personnel Services Branch (PSB), Training and Consulting Services Branch, and Acquisition and Corporate Services Branch.

We also met with officials from Division of Finance (DOF), Division of Information Resources Management (DIRM), Office of Ombudsman (OO), Office of Diversity and Economic Opportunity (ODEO), and Office of the Executive Secretary (OES), all of whom handle sensitive employee data. Moreover, we met with officials from our Office of Management and Policy. Finally, we interviewed administrative management officials in the Division of Supervision and Division of Resolutions and Receiverships to get their views and discuss their practices.

In general, we discussed the following:

- the type of employee data maintained in the division or office – both manual records and data within systems,
- physical safeguards for records or files with sensitive employee data,
- access controls for the systems with sensitive employee data,
- procedures or practices for safeguarding employee data,
- protections in place for employee data shared or maintained by contractors and third-party benefit providers, and
- their views about the vulnerability of sensitive employee data to unauthorized access and misuse.

We also reviewed:

- relevant policies and procedures and applicable laws and regulations,
- various background articles and reports about privacy and identity theft, and
- internal memoranda and the final report issued in 1996 by an FDIC internal confidentiality task force.

We decided not to test compliance with policies and procedures or controls. Our decision was based on the results of our discussions with management, other work completed by the OIG and GAO, and relevant corporate initiatives planned or underway that reflected the Corporation's desire to ensure employee data was kept confidential.[6] Had we performed detailed testing, other matters may have come to our attention.

Finally, as stated above, the scope of our work with respect to information systems was limited to discussions with officials about systems containing sensitive data and did not include testing of general controls designed to safeguard those systems from unauthorized access or data manipulation. As part of our work, we reviewed GAO's *Financial Audit: Federal Deposit Insurance Corporation's 1999 and 1998 Financial Statements* (GAO/AIMD-00-157, May 2000) and GAO's management letter issued to the Chairman about weaknesses identified in FDIC's information system controls.

Our review was conducted in headquarters from April to August 2000 according to the President's Council on Integrity and Efficiency's *Quality Standards for Inspections.*

Where is sensitive employee data?

In the course of conducting business, the Corporation creates and receives information of a confidential or sensitive nature. This includes, among other things, sensitive employee data. As with any organization, sensitive employee data is needed in many instances for administrative purposes. Specifically, FDIC uses employee SSN as an employee identification number. As discussed later, FDIC plans to use a different employee identification number when the Corporate Human Resource Information System (CHRIS) is implemented.

At the time of our review, because SSN was used as an employee identification number, supervisors, administrative officers, and timekeepers within divisions and offices were privy to confidential employee information in meeting their responsibilities when handling training requests, performance evaluations, personnel actions, and the like. In addition, employees might keep copies of administrative forms or personnel actions about themselves at their desks. Employee data is routinely maintained or processed in certain divisions such as DOA and DOF. Moreover, the health and fitness centers have sensitive medical data. ODEO and OO have other types of information that is considered sensitive to employees. Finally, third-party benefit providers and contractors might maintain or access sensitive employee data.

[6] FDIC OIG's Office of Audit has also initiated a survey *Independent Security Review of FDIC's Mainframe and Related Procedures* (Audit Project 2000-919). The objectives of that project are to assess the information system security controls over the mainframe using DIRM's independent security review procedures and to evaluate DIRM's independent security program to identify process improvement opportunities.

How is sensitive employee data handled at FDIC?

Most FDIC employees recognize and safeguard confidential information that has been entrusted to them.

1996 Confidentiality Task Force Conclusion

Corporate and division policies had been issued which set forth procedures, and employees have developed common practices, which when followed, establish an environment where sensitive data should be safeguarded. Appendix III highlights excerpts from FDIC internal guidance that addresses the need to keep employee data confidential. Some divisions and offices have developed written procedures to provide additional guidance on this matter. In addition, FDIC was taking action to ensure information system general controls were operating as intended.

At a corporate level, personnel or employee records are considered confidential and, as such, should only be disclosed to those individuals who have a need to know the information for purposes of conducting business. The Corporation and all its employees are obligated to protect confidential information. The Privacy Act of 1974 provides the overall framework for collecting and maintaining personal information about individuals. In addition, FDIC has rules that limit the disclosure of confidential information under the Freedom of Information Act.

More specifically, FDIC Circular 1031.1, *The Privacy Act of 1974: Employee Rights and Responsibilities,* provides guidance to employees about the rights and responsibilities imposed by the Privacy Act. This circular:

- establishes the Corporation's responsibilities for collecting and maintaining information, and
- recognizes that each employee will come into direct contact with information about other individuals, and that it is essential that each employee be familiar with the provisions of the Privacy Act.

The circular requires the Corporation to establish reasonable administrative, technical, and physical safeguards to assure the records are disclosed only to those who are authorized to have access. Each employee has responsibilities for preventing disclosure of information on individuals contained in Corporate systems of records unless consent for disclosure has been given. Additionally, employees are to ensure that official files retrievable by name or other identifier must be included in the Corporation's systems of records.

FDIC's procedures and practices are designed to prevent unauthorized disclosure or access to records or systems to individuals without a business need to know. Some of the general procedures and practices described to us included:

- Confining offices and divisions that handle or process significant employee data and records to limited access floors. Examples include PSB, Security Management Section, ODEO, and OIG.

- Keeping official personnel folders in PSB and the OIG's Human Resources Branch in locked file rooms and monitoring access to those files in accordance with U.S. Office of Personnel Management requirements.
- Keeping unofficial personnel files maintained by administrative officers in locked file rooms or file cabinets.
- Using sensitive document covers and folders. The purpose of these document covers or folders is to inform persons handling the documents that the documents are sensitive or confidential in nature and should only be shared with FDIC staff or authorized contractors who require the information to perform their duties. Moreover, these covers serve as a reminder that the documents need to be secured in accordance with appropriate guidance.
- Providing training to officials that routinely handle sensitive employee data and records about their responsibilities. DOA officials and the OIG's Human Resources Branch officials also told us that they were trained to safeguard personnel records. Likewise, OO, ODEO, and OES officials told us that they were trained to handle confidential information – including personally identifiable employee data – with great care. Administrative officers that we met within division and offices were aware of the need to keep unofficial personnel records and other administrative files that contain sensitive employee data in a secure environment.
- Sending reminders periodically to personnel who routinely handle sensitive information about their responsibilities to safeguard that information. For example, in February 2000, PSB issued a memorandum addressing this issue.
- Implementing clean desk policies in some offices to help ensure that sensitive information is not inadvertently left unattended.
- Evaluating safeguards over sensitive data as part of the annual Internal Control Assessment Process.
- Establishing a corporate-wide suitability program to help ensure that FDIC only employs persons who meet all Federal requirements for suitability, including character, reputation, honesty, integrity, and trustworthiness, and whose employment or conduct will not jeopardize the accomplishment of the Corporation's duties or responsibilities.

Some offices had memorialized their policies and practices in writing. In response to our question, five of the offices we contacted provided us with copies of written policies addressing the need to protect employee data--DOA, OO, DIRM, DOF, and OIG.

The Corporation had also designed safeguards to help ensure that employee data needed by contractors or third-party benefit providers was kept confidential. Specifically, the Corporation incorporated data confidentiality clauses in FDIC contracts which provided that any data a corporate contractor comes into contact with will not be subject to disclosure to any other parties except for any legal or regulatory requirements. However, we found that FDIC did not have a confidentiality agreement in place either through the policy agreement or contracting vehicle with CIGNA Corporation. CIGNA Corporation provides FDIC employees with dental insurance. As a result of our review, however, FDIC was working with CIGNA Corporation to get an agreement in place to ensure that enrollment and claim information provided to CIGNA Corporation by FDIC employees is safeguarded.

Although physical security is important, protecting hardcopies of corporate information in locked file cabinets and locked offices is no longer sufficient security when most of the original data is

on-line and accessible from at least one computer system. As we previously mentioned, in its 1999 financial audit report, GAO reported general control weaknesses over information systems. The Corporation has stated that it will continue information system improvement efforts and will take corrective actions to address the issues and recommendations reported by GAO.

In addition, officials we interviewed were aware of the need to limit access to systems containing sensitive employee data to those individuals with a business need to know. For example, PSB's Assistant Director, Information Systems and Services Section, described the following controls applicable to the personnel systems:

- All of the systems required Login ID and were password protected.
- There were also levels of authority granted to authorized users – some users were granted read only access or could only update certain fields or data elements.
- Systems only appeared on the desktops of authorized users.

The Assistant Director, Information Systems and Services Section, also told us that access controls over all personnel systems had improved as a result of corrective actions taken in response to a 1999 OIG audit.[7] Specifically, OIG reported that FDIC needed additional procedures, processes, and controls to more fully protect personnel database files from unauthorized browsing and intentional or inadvertent unauthorized changes. In response to that report, for each of its systems, PSB completed a "scrub" of all authorized users and reviews and began updating the list of authorized users on a quarterly basis. A more recent OIG review also resulted in improved physical safeguards over confidential information collected and generated during the application process.[8]

Where is employee data potentially at risk to unauthorized disclosure or use?

The risk of identity theft can be minimized by managing personal information wisely, cautiously, and with heightened sensitivity.

Federal Trade Commission Booklet – ID Theft: When Bad Things Happen to Your Good Name

Despite the procedures and practices designed to safeguard the employee data, sensitive data was potentially vulnerable to the extent that employees did not follow procedures and general information system controls were not fully implemented or operating as intended. Moreover, as mentioned in one article, ultimately, it is people who protect information, not policies. For that reason, people must understand policies and take responsibility for implementing them. To strengthen information handling practices, privacy advocates recommended (1) raising employee awareness about their responsibilities and the importance of securing sensitive information and (2) minimizing the use of the SSN on any documents widely seen by others. At FDIC, this included CTAWs.

[7] *Audit of Personnel Action Processing Controls and Security* (Audit Report No. 99-028), dated July 29, 1999.
[8] *Internal Controls Over Confidential Information Collected and Generated During the Application Process* (Evaluation Report No. 00-003), dated March 24, 2000.

Officials we met with acknowledged that individuals might be careless, at times, in handling forms, reports, or records that contain sensitive employee data. Our discussions with officials indicated that this inadvertent carelessness could be attributed to two factors: (1) the use of employees' names and SSNs for administrative purposes and (2) the lack of awareness about the reported incidents of information being mishandled at FDIC. In short, employees might not always think about how often they provide this information or handle documents of this nature.

For example, an employee might have copies of personnel action forms, time and attendance reports, or benefit forms in a file drawer or on their desk, but leave the office and file drawer unlocked. Likewise, an employee might complete a training authorization form and place it in the training coordinator's mailbox without putting the form in an envelope. In both cases, sensitive employee data is at risk and steps could easily be taken to limit access to that information. Employees might not always properly dispose of documents with sensitive data. Policies and common sense dictate that these type of documents be shredded. Privacy advocates recommend that employees be reminded about their responsibilities to safeguard documents with sensitive information. Consequently, employees need to understand the importance of securing this type of information whether it is sensitive information about themselves or fellow employees.

In response to recent indictments of government employees, including an FDIC employee, the OES issued a global Email on August 17, 2000, that was designed to raise awareness about what information is considered to be sensitive and confidential in order to prevent the inadvertent disclosure of such information. OES also posted questions and answers about the confidentiality of records on its web page on the FDICnet. This page also has links to related Email messages on identity theft and privacy of electronic communication. Specifically, on June 14, 2000, DCA issued an Email that provided information about identity theft. This Email provided employees an opportunity to learn how to minimize the risk of being a victim of identity theft. DOA's Security Management Section also periodically sends security reminder Emails to all employees.

When asked about where employee data was vulnerable, officials we interviewed consistently responded CTAW. Employee name and SSN are included on CTAW to ensure record accuracy and for identification purposes. Officials were concerned because they had observed in many instances that these forms are unwittingly left unattended in either in-boxes or on the desks of employees, supervisors, or timekeepers. Consequently, officials believed that these forms potentially could be seen by others who otherwise should not have access to this information.

Privacy advocates have suggested that the use of SSNs for record keeping purposes and personal identifiers be strongly discouraged. Moreover, when SSNs are used, organizations should have strict policies prohibiting the display of SSNs on documents that are widely seen by others – one example being time cards. During our review, FDIC used the employee's SSN as the employee identification number, but planned to use an alternative number when CHRIS was fully implemented.

With respect to other forms, DOA's Directives and Forms Management Group, the Legal Division, and OES routinely work together to help ensure that such things as employee name, SSN, or other information are only collected when there is a legitimate need to do so. This is

done as part of FDIC's responsibilities under the Privacy Act.[9] Specifically, OES and Legal Division officials review forms to ensure the proper Privacy Act notice is included on forms that do collect sensitive employee data.

Some offices had implemented measures to protect CTAWs during processing. For example, in one office, we were told that CTAWs were kept in file folders as they were routed through the supervisor and timekeepers. Other offices established a clean desk policy to help ensure that documents were not inadvertently left unattended. DOF was piloting the use of locked in-boxes in headquarters to help ensure that employees' CTAWs were kept secure until processing began.

The scope of our work did not include evaluating the specific handling practices of CTAWs in each office. However, in light of concerns raised, we discussed with officials in PSB and DIRM the possibility of reprogramming CTAW to partially or fully mask employees' SSNs when the form is printed. We were told that this could be done technically, but PSB would need to study the impact it would have on timekeepers who may rely on the SSN printed on the CTAW to input data into the Biweekly Time and Attendance system. Officials were also concerned about the costs to reprogram CTAW. In addition, we were told that PSB was currently evaluating a new time and attendance software package that would improve the time and attendance process and eliminate the paper-based CTAW. Thus, PSB preferred to wait until it had completed its assessment of the new software before considering interim measures that might not prove to be cost beneficial.

What more can FDIC do?

Aside from existing policies and practices, we recognized that several Corporate initiatives planned or underway were aimed at reducing the routine use of sensitive employee data and increasing employee awareness about the importance of safeguarding sensitive data about themselves or fellow employees. Specifically, as we have mentioned, the Corporation:

- was working with CIGNA Corporation to establish a confidentiality agreement,
- had completed a review of forms to ensure that Privacy Act notices are placed where required,
- was working to improve information system general controls,
- was planning to create new employee identification numbers with the implementation of CHRIS,
- was evaluating options for replacing CTAW in the near term, and
- had issued global Emails about identify theft and employee responsibilities with respect to disclosure of confidential information.

In addition, the Assistant Director, Security Management Section, told us that a new working group would be formed that would focus on document security at FDIC. We discussed the goal of the working group and the results of our work and the findings of the 1996 confidentiality task force. We offered to participate in that task force in any way deemed appropriate.

[9] The Privacy Act requires that agencies provide Privacy Act notices to inform individuals of the authority for the solicitation of information, whether disclosure of the information is mandatory or voluntary, the principle purposes for which the information will be used, the routine uses to be made of the information, and the effects, if any, of not supplying all or part of the information.

Nevertheless, we believed routine reminders were the key to maintaining employee awareness about the importance of this issue. Moreover, this measure was consistent with the confidentiality task force recommendation that a confidentiality culture should be reinforced and reemphasized over time at the Corporate level. DOA representatives agreed. To that end, we recommended the Director, DOA, have the Assistant Director, Security Management Section:

1. Send periodic reminders to all Corporate employees about the importance of keeping sensitive data safeguarded during everyday operations and in personal records. We suggested this message remind employees about the need to:

- secure their personal files that may contain sensitive data in their own workspace,
- follow existing policies and practices with respect to security and disclosure of confidential information, and
- properly dispose of confidential information in accordance with relevant guidance.

In addition, to ensure that concerns raised about CTAW were addressed until more permanent measures were implemented, we recommended the Director, DOA:

2. Reevaluate our suggestion to fully or partially mask SSNs on CTAW if the time and attendance software package being considered proved not to be a viable option for the Corporation or was not implemented for an extended period of time.

PSB's Assistant Director, Information Systems and Services Section, agreed that this option should be reevaluated. We also suggested that the Director, DOA, consider raising this issue with the Privacy Advisory Group once it was formally established. A discussion in that forum may generate other options that we might not have considered.

Corporation Response and OIG Evaluation

We received a written response from the Director, DOA, dated October 10, 2000, addressing our recommendations. Overall, DOA management officials agreed with our recommendations. The response provided the requisite elements of a management decision for each of the recommendations. The written response is included in its entirety in Appendix I. Appendix II presents our assessment of the response to the recommendations and shows that we have a management decision for each of the recommendations.

In closing, given the rising concerns about privacy, my office remains committed to monitoring the impact of privacy-related issues on the Corporation. Please let me know if you are interested in having my office do additional work to more fully address any of the issues discussed in this report, or look into any other privacy concerns you may identify. We appreciate the assistance your staff provided us during our review. If you would like to further discuss the results of our review, please call me at (202) 416-4217.

Attachments

Corporation Comments

FDIC
Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, DC 20429
Division of Administration

October 10, 2000

MEMORANDUM TO: Stephen M. Beard
Assistant Inspector General
Office of Congressional Relations and Evaluations
Office of Inspector General

FROM: Arleas Upton Kea
Director, Division of Administration

DATE:

SUBJECT: Management Response to Draft Report: *Review of FDIC's Information Handling Practices for Sensitive Employee Data*

The Division of Administration (DOA) has completed its review of the draft report issued by the Office of the Inspector General (OIG) entitled *Review of FDIC's Information Handling Practices for Sensitive Employee Data*. DOA appreciates the intensive study performed by the OIG and the recognition that several Corporate initiatives planned or underway are aimed at reducing the routine use of sensitive employee data and increasing awareness about the importance of safeguarding this data.

We agree with the conclusions of the OIG study and will move promptly to enhance the information handling practices for sensitive employee data. The report provides us with the necessary information to continue our efforts to perform effective improvements to existing controls.

Management Decision:

Recommendation 1: Send periodic reminders to all Corporate employees about the importance of keeping sensitive data safeguarded during everyday operations and in personal records. We suggest this message remind employees about the need:

- to secure their personal files that may contain sensitive data in their own workspace,
- to follow existing policies and practices with respect to security and disclosure of confidential information, and
- to properly dispose of confidential information in accordance with relevant guidance.

Management Response 1: DOA Management concurs with the recommendation. DOA, Security Management Section (SMS) will remind all employees periodically of the need to keep sensitive/confidential documents safeguarded during everyday operations. A reminder will be sent via global e-mail to all employees within 60 days of the issuance of the OIG's Final Report.

Corporation Comments

Recommendation 2: Reevaluate our suggestion to fully or partially mask SSN on CTAW if the time and attendance software package being considered does not prove to be a viable option for the Corporation or will not be implemented for an extended period of time.

Management Response 2: DOA concurs with the OIG's recommendation. By October 31, 2000, DOA, PSB will reevaluate the OIG suggestion to mask the social security number on the Corporate Time and Attendance Worksheet.

If you have any questions regarding the response, our point of contact for this matter is Andrew O. Nickle, Audit Liaison for the Division of Administration. Mr. Nickle can be reached at (202) 942-3190.

cc: Mr. Deshpande

Management Response to Recommendations

This table presents management responses to recommendations in our report and the status of management decisions. Management's written response to our report provided the information for management decisions.

Rec. Number	Corrective Action: Taken or Planned	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
1	DOA's Security Management Section will remind all employees of the need to keep senistive/confidential documents safeguarded during everyday operations via a global e-mail.	December 10, 2000	Global E-Mail	No	Yes
2	DOA, PSB will reevaluate OIG's suggestion to mask the social security number on the Corporate Time and Attendance Worksheet.	October 31, 2000	Memorandum Reporting on Results of Evaluation	No	Yes

FDIC Internal Guidance Regarding the Handling of Sensitive Employee Data

This table highlights excerpts from FDIC internal guidance that addresses the need to keep employee data confidential.

Reference	Relevant Highlights
The Privacy Act of 1974: Employee Rights and Responsibilities Circular 1031.1 **Dated 03/29/89**	• Privacy Act provides rights to and imposes responsibilities on each FDIC employee. Because of wide-ranging impact it is essential that each employee be familiar with its provisions. • Corporation is responsible for maintaining in its systems of records only such information necessary and relevant to a function that the Corporation is required to perform. The Corporation is also responsible for establishing reasonable administrative, technical, and physical safeguards to assure that records are disclosed only to those who are authorized to have access. • Each employee is responsible for ensuring that no record contained within a system of records is disclosed to any person or to any agency outside the Corporation without prior written consent of the individual who is subject to the record. There are exceptions to disclosure rules – disclosures may be made to Corporation employees who have a "need to know" the information in the performance of their duties – under one of the routine uses published by the Corporation for a particular system of record. • Privacy Act allows each individual to have access to records kept about him or her. This is especially important because the majority of the Corporation's systems of records are about Corporation employees.
Official Records and Personal Papers **Circular 1210.11** Dated 09/22/87	• Purpose is to provide policy, procedures, and guidelines applicable to the handling of official records and personal papers by Corporation officials and employees. • Personal use of Extra Copies of Official Corporation Records -- retention of extra copies must not "Violate confidentiality required by national security, privacy or other interests protected by law." • Officials and employees must not remove official records from the files. This material is in their custody for official purposes only.
FDIC Records Management Program **Circular 1210.18** Dated 05/28/97	• To establish policies and procedures governing FDIC's records management program • Exempt records as defined in 12 C.F.R Part 309 (and FDIC Rule §309.5 to include personnel, medical and similar files) shall be maintained as confidential by all present and former employees and may not be released outside the FDIC without written authorization as provided in Part 309. • FDIC employees shall ensure that their files are complete and accessible only to authorized individuals by implementing their division or office guidelines for securing confidential information.

FDIC Internal Guidance Regarding the Handling of Sensitive Employee Data

FDIC Forms Management Program **Circular 1213.1** 10/20/94	• Document Management Section is responsible for ensuring that all FDIC forms subject to a Congressional act or a management information requirement (e.g., Paperwork Reduction Act, Privacy Act of 1974, etc.) are coordinated and approved by the proper authority. • OES controls research and provision of Privacy Act Statements on those forms which request information on an individual and are maintained and retrieved using a personal identifier (i.e., Social Security number).
Data Stewardship **Circular 1301.3** 05/11/95	• To promote reliable information and to ensure data availability to clients, as needed, throughout the Corporation. • Data sensitivity establishes the basis for how data will be protected from unauthorized disclosure or alteration, or loss of use. • Data stewards serves as the source of information for data definition and protection. • Data stewards will define rules, which designate who can create, update, delete, and retrieve data. • Data stewards will work with DIRM Data Administrative Unit and Security Administration Section to identify data sensitivity levels.
Information Technology Security Risk Management Program **Circular 1310.3** Dated 11/24/97	• Establishes a program that identifies the Corporation's general support systems and major applications. • Establishes a framework for determining security risks and control requirements, and provides for their independent review and management authorization. • The Corporation has a responsibility to assess the capabilities of these general support systems and major applications to protect the confidentiality, integrity, and the availability of sensitive data they process. • Sensitivity categories will provide security commensurate with the applications perceived risk, thus ensuring that required security measures will be practical and cost-effective. • Vulnerabilities are the ways in which an application or system may fail or be attacked. They include – unauthorized access to sensitive data or information. • The Directive defines the roles and responsibilities for implementing the corporate-wide Risk Management Program.
Internet Access and Acceptable Uses **Circular 1351.3** 09/02/94	• Establish policies, guidelines, and responsibilities for access to and acceptable uses of the Internet at the FDIC. • Employees are required to be aware of computer security and privacy concerns and to guard against computer viruses and security breaches of any kind. • All employees who use the Internet will not send any sensitive information without prior approval from the appropriate managers, data stewards, and DIRM's Security Administration Section.

FDIC Internal Guidance Regarding the Handling of Sensitive Employee Data

Automated Information Systems (AIS) Security Policy **Circular 1360.1** Dated 12/23/96	• Establishes policy and assigns responsibilities for ensuring adequate levels of protection for FDIC automated information systems and the information processed, stored, or transmitted by them. • Automated information security addresses three aspects of information – confidentiality, integrity, and availability. • Sensitive information is defined to include records about individuals requiring protection under the Privacy Act, and information not releasable under Freedom of Information Act. • Sensitive information will be protected from unauthorized modification, destruction, or disclosure, whether accidental or intentional, through the use of appropriate technical, administrative, physical, and personnel controls. • Access to sensitive information and information systems will be based on business needs. • FDIC and contract personnel who work in sensitive positions (i.e., positions that entitle the incumbent to access to sensitive information) will undergo appropriate suitability checks.
FDIC Information Security Officer's Handbook **Circular 1360.7** Dated 12/21/95	• To publish automation security policies. • Security Administration Section (DIRM-SAS) is responsible for developing and implementing automation security policies and procedures. • All FDIC information Security Officers are responsible for requesting and monitoring access on behalf of employees within their scope – reporting violations of computer security to SAS.
Data Sensitivity **Circular 1360.8** Dated 05/19/95	• Defines attributes of sensitivity applicable to automated corporate data. • Data sensitivity is defined to be the characteristics of data that determines the protection requirements needed to address unauthorized disclosure, alteration, or loss of use. • Data sensitivity levels are confidential, integrity, and availability. • Nonpublic information – it includes information that he/she knows, or reasonably should know is designated as confidential by an agency. • Data with a confidentiality level of Official Use or Limited Official Use shall be disseminated only on a need-to-know basis. • Individual users shall ensure that protection of replicated data remains commensurate with its confidentiality level.

FDIC Internal Guidance Regarding the Handling of Sensitive Employee Data

Access Control for Automated Information Systems **Circular 1360.15** Dated 03/24/00	• Established the policy and roles and responsibilities for managing access to FDC Automated Information Systems (AISs) and data. • Management systems are in place to track access requests, and maintain user access profiles and authorization histories. • Access to sensitive AISs and data shall be protected from unauthorized access, disclosure, and use. • Access will be terminated when no longer required or when access privileges have not been used for a predetermined period of time. • Information Security Officers administer access authorization and local termination actions and review access control related to security reports. • Sensitive data is defined to include data covered by the Privacy Act. • Sensitive system – automated information system that requires protection because it processes sensitive data.
Personnel Suitability Program **Circular 2120.1** 09/24/99	• Informs management officials and employees of Corporation's policy regarding the Personnel Suitability Program. • Suitability program has established personnel security policies and procedures to assure an adequate level of security for the Corporation's automated information systems. These policies include requirements for screening all individuals having access to sensitive data. • The Security Management Section maintains investigative files in a secured area, separate from personnel records. Information contained in these files shall be used and disseminated only in accordance with the Privacy Act, and only authorized personnel shall have access to these records; disclosure to officials in the Corporation shall be made only on a need-to-know basis and all such disclosures shall be documented. • Reports of Investigation are part of the U.S. Office of Personnel Management record system and are subject to the routine uses listed in the Federal Register for that record system.

FDIC Internal Guidance Regarding the Handling of Sensitive Employee Data

Time and Attendance Reporting **Circular 2300.5** Dated 10/31/97	• GAO regulations require that a daily record keeping system be established. • DOA is responsible for time and attendance (T&A) program management including development of policy. DOA headquarters is the data steward for Biweekly Time and Attendance (BTA) System. • DIRM is responsible for: maintaining and protecting data files from unauthorized access, and ensuring that data is completely and accurately processed. Coordinating and forwarding to DOA all requests to add or delete timekeepers' access to the BTA system. • Timekeepers responsible for: receiving all approved T&A documents and reports from the supervisor, and filing all original documents in a locked file cabinet -- protecting T&A data files from unauthorized access and modification -- retaining the records in a locked file cabinet – maintaining strict confidentiality, log on/passwords for security purposes, and routinely logging out of the BTA system when leaving their work area. • Supervisor is responsible for – maintaining confidentiality of employees' T&A information. • Designated Auditor is responsible – retaining audit files for six (6) years**,** in addition to the current year, in a locked file cabinet. • Division and Office directors, or their designees are responsible for – providing an adequately controlled environment for collecting and reporting employees' daily T&A data. • Information Security Officers responsible for coordinating and forwarding to DOA all requests to add or delete timekeepers' access to the BTA System. Establishing passwords for timekeepers to access that portion of the FDIC mainframe system where the BTA system resides. Suspending and reinstating timekeepers' access.
Public and Confidential Financial Disclosure Reports and Other Related Employee Ethics Forms Required to be Filed **Circular 2410.2** Dated 02/21/97	• The Confidential Financial Disclosure Reports and other employee related forms are confidential and required to be withheld from the public. The forms contain sensitive commercial and financial information as well as personal information, which is exempt from disclosure. All forms and related documents, which comprise the ethics system of records, are to be stored in locked cabinets or in locked offices.

FDIC Internal Guidance Regarding the Handling of Sensitive Employee Data

New Employee Orientation Program Policy **Circular 2600.3** Dated 10/15/98	• Provides policy and procedures to FDIC Managers and Supervisors on the New Employee Orientation Program. • Appendix D – Supervisor's Checklist includes among the items to be discussed with the new employee -- the Privacy Act and also administrative issues specific to the local office including the protection of sensitive information. • Appendix E Telephone/Computer Security Information discusses do's and don'ts for passwords, e-mail and diskettes. • Appendix G Safeguarding Information Technology Assets emphasizes safeguarding security over IT equipment, especially laptops.

FDIC Employee Assistance Program (EAP)
Circular 2821.1
Dated 07/07/99
	• Informs FDIC employees of the responsibilities and functions of the FDIC Employee Assistance Program (EAP).
	• The objectives are to:
	  • Assist employees with problems related to daily life.
	  • FDIC managers and supervisors in identifying and appropriately dealing with employees who are experiencing a decline in job performance and/or conduct as a result of personal problems.
	• "The supervisor should maintain any information received from an EAP counselor or a treatment provider about the employee in a confidential manner."
	• "CONFIDENTIALITY: Counseling discussions are confidential and cannot be disclosed without the employee's written permission as provided by form FDIC 2800/27, Authorization to Release Information. Confidential communication can only be divulged without a written release from the employee when serious intent of suicide, homicide, child or elder abuse is assessed."

Official Mail **Circular 3130.11** Dated 02/12/93	• Discusses responsibilities, guidelines and procedures relating to the Corporation's official mail operations: • For confidential material – use FDIC Messenger envelopes or affix plain labels to large plain envelopes or Jiffylite insulated bags.
Disposition of Excess Computer Equipment **Bulletin 3200** Dated 10/23/99	• Establishes interim policy, procedures, and responsibilities related to the disposition of excess computer equipment. • DIRM, Client Services Branch shall: Identify excess computer equipment, clean hard drives so that no data or software remain, and release the equipment to ACSB Property Management Official.

FDIC Internal Guidance Regarding the Handling of Sensitive Employee Data

Modem Line Security **Policy Memorandum 98-001**	• Centrally managed modem pools shall be used in preference to individual modem lines. Individual outbound or inbound modem lines are permissible provided they serve a justifiable FDIC business need that cannot otherwise be met and employ adequate security precautions. • Centrally managed modem pools shall be configured for outbound service only. • Upon user session completion the connection will be dropped. • Audit logs shall be employed to provide monitoring capability.
Personal Computer Information Security **Policy Memorandum 98-010**	• Establishes the policy and standard for personal computer information security at FDIC. • Users of FDIC supplied systems shall take appropriate measures to provide for added security for their assigned personal computer systems. Measure include screen savers with keyboard locking or turning off the PC when leaving unattended, safeguarding passwords, and avoiding making sensitive information available across the network without proper controls.