

---

# FDIC'S PRIVACY AND SECURITY NOTICES –

Requirements and Policy Statements on the Internet and Intranet

Office of Inspector General  
Office of Congressional Relations and Evaluations  
May 19, 2000  
Evaluation Report No. 00-004



## REPORT HIGHLIGHTS

**Privacy and Security Notices at FDIC.gov.....12**

**FDIC's Privacy Policy Statement Was Generally Consistent with Guidance, But More Links to the Privacy Policy Statement Are Needed**

**Privacy and Security Notices at FDICnet.....17**

**No Requirement Exists for Employee Privacy Policy, But Experts Favor the Practice**

**FDIC Should Consider Establishing a Corporate Focal Point for Privacy .....23**

**Corporation Comments.....26**

## LETTER FROM THE DIRECTOR

**Date:** May 19, 2000

**To:** John F. Bovenzi  
Deputy to the Chairman and Chief Operating Officer

Chris Sale  
Deputy to the Chairman and Chief Financial Officer

William F. Kroener, III  
General Counsel

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

Privacy has been and continues to be of significant concern to the public and the Congress. This was the first in a series of reviews that we plan to conduct covering privacy-related issues. As you know, the Corporation must be sensitive to privacy issues on several levels – as a government agency – in its capacity as a regulator of financial institutions – and as an employer.

Given the heightened concerns about online privacy and, in particular, the disclosures made about information collected from visitors to web sites, we decided to concentrate our first review on FDIC's web site disclosure statements. Specifically, our objective was to determine whether the content and placement of web site privacy and security disclosure statements on FDIC's external and internal web sites met applicable disclosure requirements and concerns, and if not, what action FDIC was taking to address those matters. Further, consistent with the mission of our office, we undertook this review to identify emerging issues that may warrant management's attention. In fact, we identified one issue we believed warranted your attention and further study.

To accomplish our objective, we researched existing and evolving disclosure requirements and practices, interviewed FDIC and external officials that were knowledgeable about privacy policy requirements, and lastly, used the information obtained to evaluate FDIC's existing external and internal web privacy and security policies.

FDIC's external web site had a *Privacy Policy Statement* that described its information handling practices. We found that the content of FDIC's *Privacy*

*Policy Statement* on its external web site was substantially consistent with applicable guidance. We believed this was noteworthy because FDIC's *Privacy Policy Statement* was developed and posted on its external web site in 1998 – before any requirement to do so. FDIC's *Privacy Policy Statement* only lacked one of the recommended language elements included in the Office of Management and Budget 1999 policy guidelines. Specifically, it lacked security, intrusion, and detection language. However, we found that FDIC's *General Disclaimer* included this type of language. In addition, we found that more links were needed to the *Privacy Policy Statement* to fully comply with the requirements. Moreover, we determined that awareness of disclosure requirements might have been limited among FDIC Webmasters and Internet Coordinators.

Internally, there was not a requirement to post a clearly labeled privacy policy statement for employees on FDIC's internal system and FDIC had not done so. However, privacy experts are recommending that employers post a visible banner addressing employee privacy expectations as well as security concerns. In addition, some agencies, including the Department of Justice, have begun to visibly post such notices on their systems. FDIC believed that its existing policies provide adequate notice to employees. Nevertheless, additional reminders regarding the written procedures would further enhance FDIC policies.

In summary, we made recommendations designed to ensure that FDIC's external privacy policy is placed where required through increased awareness of key employees and strengthened procedures. In addition, we recommended that FDIC create and post a policy notice for its internal system. We believed adding a succinct policy statement where employees could regularly see it was a prudent step and consistent with the notice principle and disclosure framework established for external web sites.

Finally, we identified a matter we believed warranted further study by the Corporation. In short, we found that private sector entities and some federal agencies are establishing privacy focal points. At the federal level, these officials are distinct from the Privacy Act Officer. We recommended that FDIC examine the need for a corporate official or committee of officials who would serve as a focal point and coordinate the Corporation's privacy-related activities, many of which fall outside the parameters of those typically handled by the Privacy Act Officer.

On May 15, 2000, we received a written response from the General Counsel addressing recommendations 1 and 6. On May 17, 2000, the Director, Division of Information Resources Management provided a written response to recommendations 2 through 5. Overall, both the General Counsel and Director agreed with the findings and recommendations. The responses provided the requisite elements of a management decision for each of the recommendations. The written responses are included in their entirety in Appendix I. Appendix II

presents our assessment of the responses to the recommendations and shows that we have a management decision for each of the recommendations.

Stephen M. Beard  
Director, Office of Congressional Relations and Evaluations  
Office of Inspector General

## Table of Contents

<b>Letter from the Director</b>	1
<b>Background</b>	5
<b>Objective, Scope, and Methodology</b>	9
<b>Privacy and Security Notices at FDIC.gov</b>	12
✓ Applicable Guidance from OMB	12
✓ Content of FDIC's <i>Privacy Policy Statement</i> Was Generally Consistent with OMB Guidance	13
✓ Additional Links Needed to FDIC <i>Privacy Policy Statement</i>	15
<b>Privacy and Security Notices at FDICnet</b>	17
✓ No Requirement Exists for Employee Privacy Policy Statement, But Experts Favor the Practice	17
✓ Succinct Notice of Existing Employee Privacy and Security Policies Needed	19
<b>FDIC Should Consider Establishing a Corporate Focal Point for Privacy</b>	23
<b>Corporation Response and OIG Evaluation</b>	25
<b>Appendix I: Corporation Comments</b>	26
<b>Appendix II: Management Response to Recommendations</b>	30
<b>Appendix III: FDIC's External Web Site <i>Privacy Policy Statement</i></b>	32
<b>Appendix IV: CIO Council's Proposed Security Notice</b>	34

## Background

Throughout government there is a shared realization that rapid advances in technology, interconnectivity, and expanding usage of the Internet increases the need for and priority on adequate security and privacy measures.

### **Chief Information Office Council Fiscal Year 2000 Strategic Plan**

Recent studies have shown that privacy is the number one concern of those using the Internet. Web sites are a powerful tool for providing information on activities, objectives, policies, and programs of federal agencies and privacy has become a critical issue to the development of web sites. With the traditional concerns of government surveillance and use of personal information, federal agencies need to be particularly vigilant in addressing privacy issues. In fact, the Privacy Act of 1974 was intended to balance the government's need to maintain information about individuals and an individual's right to be protected against unwarranted invasions, maintenance, use, and disclosure of personal information by federal agencies. However, legislators did not anticipate the advent of the Internet when the Privacy Act was created.

Accordingly, creating information collection guidelines and standards on the World Wide Web has been a consistent problem for the federal government since its agencies started creating web sites. The Office of Management and Budget (OMB) and General Services Administration (GSA) issued memoranda specifically to address this issue.<sup>1</sup> In 1998, GSA issued a memorandum for Chief Information Officers and Federal Webmasters outlining *Top Privacy Principles for Federal Web Sites*. GSA's privacy principles are highlighted on the next page. GSA's memorandum suggested that a privacy notice is needed for the web site as a whole to cover web site issues such as logs, E-mails to the Webmaster, and other web site issues. The memorandum further stated that the emerging practice is to provide a button on the initial home page which provides a central location for various disclaimers and legal notices.

---

<sup>1</sup> OMB has overall responsibility for privacy information and provides guidance on privacy in OMB Circular A-130, *Management of Federal Information Resources*. GSA's Office of Information Technology issued the memorandum on privacy principles. The Office of Information Technology is responsible for promoting the strategic management and effective use of Federal information technology through collaborative development of governmentwide programs.

### **Privacy Principles for Federal Web Sites**

1. Place a high priority on protecting the public's privacy at federal web sites.
2. Stay up-to-date on the impact that changes in web site technology have on privacy.
3. Notify the public using an appropriate privacy notice whenever you are collecting data on the Internet.
4. Use information only for the purpose for which it was gathered as disclosed in the privacy notice.
5. Protect privacy for all forms of data (text, graphics, sound, and video).
6. Balance the Freedom of Information Act and the Privacy Act of 1974.
7. Information obtained to conduct system administration functions must still be protected.
8. Involve and coordinate with the agency's privacy officer when developing applications using the Internet.

#### **GSA Memorandum *Top Privacy Principles for Federal Web Sites***

In 1999, OMB issued a memorandum, *Privacy Policies on Federal Web Sites*, to the Heads of Executive Departments and Agencies directing agencies to post clear privacy policies on World Wide Web sites, and provided guidance for doing so. A privacy policy is generally a comprehensive disclosure describing the general or on-line policies and practices related to the collection and use of information. These privacy policy statements are designed to ensure that individuals have notice and choice about, and thus confidence in, how their personal information is handled when they use the Internet.

These privacy policy statements are also designed to accommodate the unique nature of web sites that the Privacy Act did not consider. For instance, the Privacy Act requires agencies to provide a Privacy Act notice to each individual from whom it collects information, which is stored in a system of records, keyed to a personal identifier or other identifying symbol assigned to an individual.<sup>2</sup>

However, according to OMB's memorandum, a large fraction of federal web pages have not collected significant amounts of identifiable information in ways that entered directly into systems of records covered by the Privacy Act. Mindful that federal agencies must protect an individual's right to privacy when they collect personal information, OMB is requiring federal web sites to include a privacy policy statement, even if the site does not collect any information that results in creating a Privacy Act record.

In the private sector, there is no requirement that entities post a privacy policy statement on their web sites, but more firms are voluntarily doing so. In fact, 1999 studies looking at whether top private sector web sites post privacy statements revealed that most sites have privacy policies posted. In comparison

---

<sup>2</sup> 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.

to similar studies done in 1997 and 1998, the private sector showed marked improvement. The 1999 studies also point out that policy statements do not always include all the necessary elements that should be included based on fair information practices.

FDIC, in cooperation with other federal bank and thrift regulatory agencies, also conducted a survey of the Internet privacy policies of insured depository institutions during May and July 1999. The survey revealed that many institutions are taking responsible, voluntary strides toward addressing the public's privacy concerns. However, the survey results also indicated that the industry can and should do more in this area.

Privacy policy statements address one of the fundamental fair information practices – the principle of notice. The National Information Infrastructure Task Force described this principle in 1995.

### **Notice Principle**

Information users who collect personal information directly from the individual should provide adequate, relevant information about –

- why they are collecting the information;
- what the information is expected to be used for;
- what steps will be taken to protect its confidentiality, integrity, and quality;
- the consequences of providing or withholding information; and
- any rights of redress.

***Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information***

Another aspect of privacy to be considered in light of emerging technology involves employee privacy. Indeed, GSA's 1998 memorandum indicated that the privacy rights of employees must also be considered in the development of web sites for Intranets. In short, new technologies make it possible for employers to monitor employees' use of electronic equipment. For instance, more companies are beginning to monitor employees' use of the Internet. Privacy advocates acknowledge that employers have a legitimate interest in monitoring work to ensure efficiency and productivity. Employers also need to ensure that employees act responsibly and use these technologies with care, otherwise computer security and corporate confidential and proprietary information could be compromised resulting in substantial loss. However, unless employees are alerted – given notice, for example – to monitoring, it could be considered by employees and the courts to be a violation of employees' reasonable expectation of privacy.



In this context, FDIC must address privacy on three levels:

- as a government agency with a public web site;
- as a regulator charged, in part, to monitoring how financial institutions address this issue; and
- as an employer with an Intranet.

## Objective, Scope, and Methodology

This review was one in a series of reviews we plan to conduct on privacy-related topics. The objective of this review was to determine whether the content and placement of web site privacy and security disclosure statements on FDIC's external and internal web sites meet applicable privacy and security-related disclosure requirements and concerns, and if not, what action FDIC is taking to address those matters. Consistent with the mission of our office, we undertook this review not only to provide assurance that FDIC's existing policies and practices are consistent with applicable guidance, but also to identify emerging issues that may warrant management's attention.

To accomplish our objective we:

- ✓ Interviewed officials from the OMB, GSA Office of Governmentwide Policy, and the Chief Information Officers (CIO) Council.<sup>3</sup> Our research indicated that these officials were knowledgeable about governmentwide policies on privacy and security.
- ✓ Researched privacy-related topics on the Internet to yield articles and issue papers relevant to our review.
- ✓ Identified and reviewed the following guidance for federal agencies:
  - OMB Memorandum 99-18 *Privacy Policies on Federal Web Sites* dated June 2, 1999,<sup>4</sup>
  - GSA Memorandum for Chief Information Officers and Federal Webmasters on *Top Privacy Principles for Federal Web Sites* issued in 1998,
  - GSA Office of Governmentwide Policy Memorandum, *Model "Limited Personal Use Policy" of Government Equipment* dated June 7, 1999, and
  - National Information Infrastructure Task Force paper entitled *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* dated June 6, 1995.
- ✓ Discussed the development of FDIC's *Privacy Policy Statement and General Disclaimer* and relevant FDIC policies and procedures with officials in the Division of Information Resources Management (DIRM), Legal Division,

---

<sup>3</sup> The CIO Council is the principal interagency forum to improve the design, modernization, use, sharing, and performance of Information Technology resources.

<sup>4</sup> We did not ask FDIC's Legal Division to formally opine whether FDIC was required to comply with OMB's memorandum because DIRM officials told us it was their intent to comply regardless of its statutory applicability to the Corporation.

Office of the Executive Secretary (OES), Division of Compliance and Consumer Affairs (DCA), and Office of Corporate Communications.

- ✓ Reviewed relevant FDIC policies, including:
  - Circular 1370.3, *Use of Electronic Communications*, dated August 6, 1997,
  - Circular 1351.3, *Internet Access and Acceptable Uses*, dated September 2, 1994,
  - Circular 1370.4, *Publishing FDIC Information Via the Internet and FDICnet*, dated August 29, 1997,
  - Circular 1031.1, *Privacy Act of 1974: Employee Rights and Responsibilities*, dated March 29, 1989, and
  - Circular 1213.1, *FDIC Forms Management Program*, dated October 20, 1994.

Our review of FDIC's policies addressing employees' use of FDIC's computer resources was limited to the privacy aspect of those policies.

- ✓ Reviewed *FDIC Correspondence Manual* Chapter 7, *Electronic Correspondence* and DIRM's *A User's Guide to Information Security*.
- ✓ Evaluated the placement and content of FDIC's existing *Privacy Policy Statement* and *General Disclaimer* on the external home page based on the relevant guidance on privacy and security notices we identified. Specifically, we:
  - compared the language content of FDIC's policy to guidance in OMB Memorandum 99-18 and GSA Memorandum on *Top Privacy Principles for Federal Web Sites*, and
  - systematically reviewed FDIC's external web pages to test whether the required privacy policy link was located on pages where personal information was collected from the public.
- ✓ Reviewed and evaluated FDIC's disclaimers and notices posted on FDIC's Intranet (FDICnet).
- ✓ Sent a survey to 54 FDIC staff members who are designated as Division Internet Coordinators or Webmasters. The intent of our survey was to assess their knowledge of OMB's guidance for external web privacy policies and FDIC's *Privacy Policy Statement* and *General Disclaimer*. Additionally, we were interested in getting their views on posting a privacy statement for employees. We received responses from 14 of the 54 officials surveyed.
- ✓ Contacted other agencies, primarily federal banking and thrift regulatory agencies, to learn about: Internet privacy policies, Internet security and general disclaimer notices, and whether privacy and security notices were

visibly posted on their respective Intranets. Our goal in doing so was to identify best practices. Specifically, we reviewed the privacy policies posted on the principle web page for the Office of Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Federal Reserve), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA), and Department of the Treasury. The Federal Reserve also has a separate disclaimer posted that we reviewed in conjunction with its privacy policy.

- ✓ Interviewed an official at the Department of Justice to discuss the type of notice or banner posted on its internal system and rationale for doing so.
- ✓ Coordinated our review with OIG's Office of Audit, which was conducting a related review entitled *Controls Over Employee Internet Use*. The objectives of that review were to determine the adequacy of (1) FDIC's policies governing Internet use and (2) current procedures and tools used to monitor FDIC employees use of Internet resources.
- ✓ Consulted with the OIG's Office of Counsel.

During our review, OES and the Legal Division reviewed web forms to ensure that the proper Privacy Act notices were on those forms. Accordingly, the scope of our review did not include evaluating whether Privacy Act notices were included where required. However, we did consider the results of their review in evaluating issues that we believe may warrant management attention.

We conducted our review from November 1999 to March 2000 according to the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*.

## Privacy and Security Notices at FDIC.gov

FDIC's *Privacy Policy Statement* on its World Wide Web page ([www.fdic.gov](http://www.fdic.gov)) was substantially consistent with the model language provided in OMB Memorandum 99-18 *Privacy Policies on Federal Web Sites*, and with the content of privacy statements of other agencies that we contacted. However, it lacked security, intrusion, and detection language that OMB suggested agencies include in their privacy policy statements. In addition, we found the *Privacy Policy Statement* was not located on all web pages that collect personal information as required. A review of web forms done by the Legal Division and OES also found that the required Privacy Act notices were not on all web forms as required. Finally, our survey results indicated that awareness of privacy disclosure requirements might have been limited among FDIC Webmasters and Internet Coordinators.

### Applicable Guidance from OMB

The intent of a privacy policy statement is to tell visitors to the site how any information obtained from them, either automatically or voluntarily provided, is handled. As discussed in the background section, OMB's Memorandum 99-18, *Privacy Policies on Federal Web Sites*, provides guidance for creating a privacy policy statement. We also learned that the CIO Council was in the process of developing guidance to standardize security notices posted on federal web sites.

#### OMB's Privacy Policy Requirements

- Post a privacy policy statement on the principal web sites by September 1, 1999.
- By December 1, 1999, OMB directed agencies to add privacy policies to any other known, major entry points as well as at any web page where substantial personal information from the public is collected.
- Each policy must clearly and concisely inform visitors to the site
  - ✓ what information the agency collects about individuals,
  - ✓ why the agency collects it, and
  - ✓ how the agency will use it.
- Privacy policies must be clearly labeled and easily accessed when someone visits a web site.

To assist agencies in reviewing their existing privacy policies or in creating such a policy, OMB provided guidance and model language for several different information practices. OMB's memorandum stated that agencies could use the model language verbatim, or as a starting point in crafting a policy tailored to meet the agencies' own requirements. OMB's memorandum suggested that agencies include the following language in their privacy policies:

<b>Introductory language</b>	✓ Overview language about privacy practices at the start of the policy.
<b>Information collected and stored automatically</b>	✓ The policy should make clear whether or not the agency is collecting information automatically or using cookies and whether any steps will be taken to collect more information.
<b>Information collected from E-mails and web forms</b>	✓ Some statement about how identifiable information is treated when the individuals provide it through E-mail or web forms.
<b>Security, intrusion, and detection language</b>	✓ Some statement about whether the agency uses information collected on a site to detect harmful intrusions and to take action once an intrusion is detected.
<b>Significant actions where information may be subject to the Privacy Act</b>	✓ For situations where a Privacy Act notice would be required in the paper-based world, the general principle is that the equivalent notice is required in the on-line world. Posting of the relevant Privacy Act notice on the web page or through a well-marked hyperlink would be appropriate.

**Content of FDIC’s *Privacy Policy Statement* Was Generally Consistent with OMB Guidance**

FDIC’s *Privacy Policy Statement* was developed with input from DIRM, the Internet Operating Committee, OES, DCA, and the Legal Division. FDIC’s policy statement was developed and posted on the external web site in 1998. Officials reviewed the policy statement after OMB’s memorandum was issued in 1999. FDIC’s *Privacy Policy Statement* discloses the Corporation’s information gathering and dissemination practices of its web site.

Consistent with OMB’s memorandum, FDIC’s privacy policy describes what information the agency collects about individuals, why the agency collects the information, and how the agency will use the information. FDIC’s external web site *Privacy Policy Statement* is included as Appendix I. Notably, FDIC’s privacy statement includes all of OMB’s suggested model language noted above except for the security, intrusion, and detection language.

FDIC OIG and Legal Division counsel informally opined that the OMB’s guidance does not require that agencies include all the model language suggested by OMB in their respective privacy policies. DIRM officials told us that they intentionally did not include security, intrusion, and detection language in the privacy policy because this type of language is not considered to be user-friendly. In addition, they were concerned that this type of language could attract “hackers”. According to DIRM officials, if an entity advertises that it monitors for unauthorized attempts to upload information – hackers are more inclined to try.

However, FDIC’s *General Disclaimer*, also posted on its web site, contains security, intrusion, and detection language. Specifically, it states

***“This is a protected U.S. government web site. It is unlawful to intentionally cause damage to it or to any FDIC electronic facility or data through the knowing transmission of any program, computer virus, information code, or command. This system and related equipment are subject to monitoring. Information regarding users may be obtained and disclosed to authorized personnel, including law enforcement authorities, for official purposes.”***

Thus, FDIC addresses this aspect of the model language, but not as part of its privacy statement. Nonetheless, we raised this issue because we learned that the CIO Council is working on new guidance that will likely require agencies to post a separate security notice on World Wide Web sites. An official working on the project told us that the goal of the Council is to standardize the language used governmentwide. The language that the CIO Council provided to us is included in Appendix II. The proposed language is similar to the language included in FDIC’s *General Disclaimer*. However, the proposed language identifies the applicable criminal statutes that can be pursued for intentional harm caused to a web site.

We also found that FDIC’s *Privacy Policy Statement* language was consistent with that of the other agencies we contacted. Table I shows the five OMB language guidance elements and how FDIC’s *Privacy Policy Statement* compared to the privacy statements of each of the other bank regulation agencies during our evaluation.

**Table I: Comparison of Agency Privacy Policy Statements**

<b>Notices and Content</b>	<b>OCC</b>	<b>Federal Reserve</b>	<b>OTS</b>	<b>Treasury</b>	<b>NCUA</b>	<b>FDIC</b>
Privacy Policy on External Web Page	✓	✓	✓	✓	✓	✓
Other Type of Notice or Disclaimer Posted	Security	Disclaimer	Security	None	None	General Disclaimer
Introductory Language	✓	✓	✓			✓
Information collected and stored automatically	✓	✓	✓	✓	✓	✓
Information collected from E-mails and web forms	✓	✓	✓	✓	✓	✓
Security, intrusion, and detection language		✓		✓	✓	
Significant actions where information may be subject to the Privacy Act						✓

**Source: OCRE analysis of agency privacy policy statements and other notices**

## **Additional Links Needed to FDIC *Privacy Policy Statement***

While the content of FDIC's privacy policy was substantially consistent with OMB's guidance, we found that FDIC's *Privacy Policy Statement* was not located on every web page that collects personal information as required. Specifically, from FDIC's Internet home page, we systematically reviewed 61 web pages to test whether there was a link to the *Privacy Policy Statement* on web pages that collect personally identifiable information. We found FDIC's privacy policy was posted as required in 55 of 61 instances. On the six web pages where the policy was not posted, individuals were required to provide their name, address, telephone number, or E-mail address to receive information. We talked with officials at GSA and OMB knowledgeable about OMB requirements and they agreed that these items are generally considered to be personal information. Accordingly, they stated FDIC should add links to the *Privacy Policy Statement*.

We provided OES with copies of the web pages we identified. OES agreed to review the pages and verify that those pages were indeed required to be linked to FDIC's *Privacy Policy Statement*. OES also planned to evaluate whether any of those pages required a Privacy Act notice because of their ongoing work in that regard. Specifically, officials in the Legal Division and OES recently undertook a review of web forms to ensure that Privacy Act notices were posted as required. Their review found that some web forms did not include the required Privacy Act notices. Officials told us that the Privacy Act notices were subsequently added to some of the forms identified in their review. The Privacy Act Officer was researching the need for a Privacy Act notice for the remaining forms identified. The need for a Privacy Act notice is important not only to comply with the Privacy Act, as we explained in the background section, but also to ensure that FDIC's *Privacy Policy Statement* accurately reflects its practice. Specifically, FDIC's *Privacy Policy Statement* tells visitors that Privacy Act notices are posted where required.

We believed omissions of privacy disclosures could continue to occur unless FDIC strengthens procedures to ensure that officials knowledgeable of privacy-related disclosure requirements review web pages before they are posted. In addition, Webmasters and Internet Coordinators must be aware of the need for such a review. The responses to our survey of Webmasters and Internet Coordinators indicated that awareness of privacy disclosure requirements might have been limited. Specifically, 9 of the 14 respondents had reviewed FDIC's *Privacy Policy Statement*, and just 2 of the 14 respondents were aware of OMB's guidance.

FDIC had procedures in place covering the review of information before it is posted on the web. For instance, FDIC Circular 1213.1, *FDIC Forms Management Program* states that the OES in coordination with the Document Management Section ensures that forms adhere to specific public reporting requirements, including the Privacy Act. However, we noted that FDIC's Circular



1370.4, *Publishing FDIC Information Via the Internet and FDICnet*, does not specifically address the need to consider Privacy Act requirements or the external *Privacy Policy Statement*. Further, an OES official told us that officials knowledgeable about privacy-related disclosures did not always review web pages before they were published on the Internet.

Certainly, FDIC deserves credit for its efforts to date in developing and posting a privacy policy on its external web site. However, FDIC needed to take additional action to ensure that it fully complies with new mandates and that its privacy policy accurately reflects its practices. We believed this was important not simply to comply with requirements, but to help ensure the Corporation effectively deals with the number one concern of those using the Internet – privacy. Additionally, and perhaps more importantly, FDIC could lead by example in dealing with an issue that it is requiring financial institutions to address. Accordingly, we recommended that:

FDIC's General Counsel should have FDIC's Office of Executive Secretary:

1. Complete its review of web pages we identified and add any necessary links to the *Privacy Policy Statement* and any required Privacy Act notices.

The Director, DIRM, should have the Chief, Internet Publication Section:

2. Contact the CIO Council and review the proposed security notice language and determine how the Corporation will respond to the pending guidance from the CIO Council.
3. Develop guidance for Internet Coordinators and Webmasters and ensure through training or other means deemed appropriate that they are aware of privacy-related disclosure requirements of OMB Memorandum 99-18 and the Privacy Act. As appropriate, existing procedures for reviewing information posted on FDIC's Internet web site should be modified to reflect guidance developed.

To the extent necessary, the Chief, Internet Publication Section should work in consultation with OES and the Legal Division to address these recommendations.

## Privacy and Security Notices at FDICnet

At the time of our review, there was not a requirement to post a privacy policy statement for employees on Intranets. However, privacy experts believe the practice of posting a policy statement (i.e., notice or banner) on internal systems is advisable. Furthermore, we learned that some other agencies have such notices posted on internal home pages, E-mail screens, or log-in screens. We realized that FDIC had various policies addressing this issue. Nevertheless, without a visible banner or link to a succinct policy statement there was a risk that employees might not be sufficiently mindful of FDIC's policies. The presence of a banner reduces that risk by serving to remind employees of pertinent FDIC policies. FDIC officials told us they were in favor of adding a banner or notice. We believed this was a prudent action.

### **No Requirement Exists for Employee Privacy Policy Statement, but Experts Favor the Practice**

None of the external officials we interviewed were aware of any specific guidance requiring that privacy policies be posted for employees on Intranets. Officials at OMB and the CIO Council told us these issues have been discussed, but up to now, the focus has been on developing guidance for external federal web sites. Nonetheless, an official from the CIO Council told us that the security notice being developed for external web sites that we previously discussed could be used on internal systems as well.

According to articles written on the subject, posting a visible banner or notice on internal systems is an advisable practice. This practice was recommended in addition to having policies in employee manuals. The reason for posting this type of banner is to remind employees about the policies for the use of electronic equipment as well as the policies for monitoring such use. Similar to an external privacy policy, the intent of this type of notice is to assist employees in understanding the employer's data collection and information handling practices. It can also be used to remind employees about the appropriate use of electronic resources and employee security responsibilities. Applying the standards for external policy statements, the notice should be clearly labeled and easily accessed.

Courts will look at an employer's policies in determining whether employees have a reasonable expectation of privacy in their electronic communications. For example, according to an article written on the subject, violations of employee expectations of privacy whether by accessing a top desk drawer, reading files on a desk, or reading E-mail have similar consequences. If not done within the expected norms, employers risk expensive litigation and diminished employee morale. FDIC believes its policies provide adequate notice of Internet monitoring procedures such that employees cannot have an objective expectation of

privacy. Nevertheless, additional reminders regarding the written procedures would further enhance the FDIC's position.

Guidance developed by the Electronic Messaging Association for use in developing an E-mail monitoring policy is highlighted below. We found this guidance to be a good summary of what other experts suggest and believe it can be useful in developing policies for employee use of the Internet and other electronic equipment resources. Notably, one of the suggested practices is to post a notice when employees log on to the computer network.

### **Policy Guidance**

1. Develop or extend corporate policies to address employee privacy expectations.
2. Determine the extent of any current monitoring and limit monitoring to "work related" and supervisory activities. State extent of monitoring in policy.
3. Educate and periodically remind employees and management of policy.
4. Post a notice when employees log onto the computer network and require an affirmative acknowledgement by having the employees indicate that they have read the screen before moving on. The notice should state clearly that the system and e-mail are not private and will be audited and the parameters of employee use. It should also state on-line etiquette for using the network and company resources.
5. Address back-up and retention of stored mail.
6. Set forth how any accessed information will be used.

***Electronic Messaging Association***

In addition to expert opinion, two agencies we contacted had notices or visible links to their policy statements on their internal systems. Specifically, we were told that the Federal Reserve's *Internet and Automated Systems: Appropriate-Use and Privacy Policy* periodically appears on employees' screens. Employees must click a button to acknowledge that they have read the policy statement. We were also told that the Department of the Treasury's internal home page has a visible link to its Internet use policy. When using E-mail, employees see a banner appear on the screen that states E-mail should not be considered private.

An official at the Department of Justice (DOJ) stated it had a banner on the system log-in screen. The banner essentially tells DOJ employees that they should have no expectation of privacy and that the use of E-mail and Internet could be monitored. Employees are required to click a button to acknowledge the terms of the notice. According to this official, putting this notice up-front makes the most sense. The OIG's Office of Audit also found in its review of *Controls Over Employee Internet Use* that posting a notice or banner

communicating the Corporation's monitoring policy was done at other agencies and determined it to be a best practice.

### **Succinct Notice of Existing Employee Privacy and Security Policies Needed**

FDIC had a notice posted on the FDICnet home page that is highlighted below. However, this notice did not address employee use of the Internet or Intranet, privacy, or warn that only authorized users should access the system. We did not see any other notice, banner, or visible link to a privacy policy for employees posted on the FDICnet home page.

**FDICnet Home Page Notice**

“FDICnet is the Intranet for the FDIC. This network provides a secure location for posting information for the FDIC. Internal Resources are accessible through FDICnet. There are also links to external sites on the World Wide Web (WWW) to aid research. Information posted here cannot be accessed by users of the Internet. Links to sites outside of FDICnet do not imply endorsement by the FDIC. The FDIC cannot guarantee the validity of any site on the WWW. “

We also reviewed the notices posted on the FDICnet division and office home pages. We found that only a few home pages had notices. Generally, the notices were similar to the notice posted on the FDICnet home page except for the Legal Division's home page. That home page notice advised employees that information and documents presented on the Intranet contained information for internal use of FDIC personnel only. Further, the Legal Division notice states that none of the materials should be distributed to the general public without proper approval.

In addition, FDIC's *General Disclaimer* posted on the external web site ([www.fdic.gov](http://www.fdic.gov)) states that the terms “extend to the FDIC, its directors, officers, and employees”. In addition to providing a security warning as discussed earlier in the report, it also provides general notice that the FDIC's system is subject to monitoring. Employees may occasionally access FDIC's external web site through the FDICnet home page, but it is not likely they routinely do so. Moreover, there is nothing visible on the FDICnet home page to direct or link employees to the *General Disclaimer*. Thus, employees might not be sufficiently mindful that the policy statement in the *General Disclaimer* is applicable to them.

FDIC also had several policies that address employee privacy with regard to E-mail, use of the Internet and Intranet, and security issues. Employees can access these policies through the FDICnet. Table II summarizes key aspects of

these policies relative to employee privacy and employee responsibilities with respect to security.

**Table II: Privacy and Security Policy Statements Relative to Employees**

Policy	Policy Excerpts
Circular 1370.3 <i>Use of Electronic Communications</i>	<ul style="list-style-type: none"> <li>✓ The Corporation cannot guarantee that electronic communications will be private.</li> <li>✓ It is the policy of FDIC not to regularly monitor the content to electronic communication. However, the content of electronic communications and the usage of electronic communications will be monitored for the performance of operation, maintenance, auditing, security, or investigative functions. Electronic communications statistical data will continue to be collected on a routine basis.</li> <li>✓ Monitoring may also be necessary in order to comply with legal requirements that FDIC records be examined or produced, such as those of the Freedom of Information Act, court rules or court orders. Emergencies of internal security concerns reasonably necessitate such monitoring.</li> <li>✓ Use of the FDIC's electronic communications systems constitutes the user's consent to this policy.</li> </ul>
Circular 1351.3, <i>Internet Access and Acceptable Uses</i>	<ul style="list-style-type: none"> <li>✓ E-mail is not private communication, since others may be able to read or access it.</li> <li>✓ Employees are required to be aware of computer security and privacy concerns and to guard against computer viruses and security breaches of any kind.</li> <li>✓ Employees should not send any sensitive information without prior approval from the appropriate managers, data stewards, and DIRM's Security Administration Section. Be aware that Internet E-mail is not a secure communication channel.</li> </ul>
FDIC's <i>A User Guide to Information Security</i>	<ul style="list-style-type: none"> <li>✓ All information sent and received through the Internet should be considered vulnerable as it can be read and even manipulated by others. Do not send sensitive information over the Internet as it may compromise the security of the Corporation.</li> </ul>
<i>FDIC Correspondence Manual</i> chapter on Electronic Correspondence	<ul style="list-style-type: none"> <li>✓ Employees should not put anything in an E-mail message that they would not want anyone other than the intended recipient to see. For example, the manual points out that employees should not provide credit card numbers or other confidential information that could wind up in the wrong hands.</li> <li>✓ At times it may be necessary to intercept, monitor, disclose, or assist in intercepting or disclosing electronic communications. While the Corporation is committed to respecting the privacy of its employees consistent with applicable law, regulation, and policy, be aware that electronic communications can be forwarded, printed, and stored by others.</li> </ul>

Source: OIG Analysis of FDIC policies

Consistent with the notice principle and the framework for privacy policy statements for external web sites, these policies informed employees about:

- The information the agency collects about the individuals,
- Why the agency collects the information, and
- How the information will be used.

However, it could be argued that these policies were not readily apparent to employees unless they searched through FDIC's directive system.

Although we understood the importance of established policies, we believed more could be done to ensure employees are mindful of the policies. Generally, FDIC officials we interviewed agreed. An official from DIRM's Information Security Staff stated that it was important that all users be made aware of their rights and the Corporation's responsibilities regarding privacy issues. In addition, 57 percent of Internet Coordinators and Webmasters that responded to our survey favored the idea of posting a privacy policy statement on the FDICnet.

We did not evaluate the content of these FDIC's policies other than to see how employee privacy was addressed. However, these policies were evaluated as part of the OIG's review of *Controls Over Employee Internet Use*. The results of that review suggested that FDIC should strengthen its policy with respect to the use of electronic equipment. Accordingly, in conjunction with the findings of that review, we believed FDIC may want to review GSA's Office of Governmentwide Policy Memorandum, *Model "Limited Personal Use Policy" of Government Equipment* dated June 7, 1999. This memorandum provides guidance to assist agencies or departments in defining acceptable use conditions for employees personal use of Government office equipment, including information technology. With regard to privacy, GSA's model policy suggests that "Executive Branch employees do not have a right, nor should they have an expectation, of privacy, while using any Government office equipment at any time, including accessing the Internet, [sic] using E-mail.

"Any use of government communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous."

In summary, although a privacy policy notice was not required for internal systems at the time of our review, we believed FDIC needed to add a visible notice of the Corporation's privacy and security policies directed to employees. Consistent with their desire to be leaders in evolving technology-based privacy issues, DIRM officials agreed with the concept. Based on discussions with

officials in DIRM, we believed this banner or notice should appear on the FDIC log-in screen. Accordingly, we recommended that:

The Director, DIRM should have the Chief, Information Security Section:

4. Develop a notice for FDIC's internal network addressing employee privacy.

Once developed, the Director, DIRM should have the Assistant Director, Operations Branch:

5. Visibly post the notice developed by the Chief, Information Security Section on FDIC's internal network.

To address various privacy interests and security concerns with respect to employee use of computer resources, we believed DIRM officials should consult with the Legal Division in developing appropriate language to include in the notice or policy statement. We suggested the Corporation consider the following points in developing the language for the banner:

- Consistent with the framework for the external policy, the banner should tell employees the type of information the agency collects about the individuals, why the agency collects the information, and how the information will be used and include appropriate security language. The banner should also be clearly visible and easily accessed.
- The banner should clearly define for employees the level of privacy to be expected when using the Corporation's resources.

Finally, because employee privacy is directly impacted by any changes to the Corporation's current policies being contemplated as a result of OIG's review of *Controls Over Employee Internet Use*, our recommendation should be considered in conjunction with the results of that review.

## FDIC Should Consider Establishing a Corporate Focal Point for Privacy

As we point out in the background section of the report, privacy is the number one concern of those using the Internet. Privacy policies have emerged as a common vehicle that government agencies and the private sector have developed to address privacy concerns of those using the Internet. This was the focus of this review. However, another matter came to our attention that we believed warranted further consideration. Specifically, in conducting this review, it became apparent that FDIC did not have a focal point to address privacy issues outside the realm of the Privacy Act Officer. We believed it was important to raise this issue because privacy has been and continues to be of significant concern to the public and the Congress.

For example, in the context of this review, no one division, office, or official was responsible for developing or implementing FDIC's external Web site *Privacy Policy Statement*. As we discussed earlier in the report, at FDIC, a team consisting of officials from DIRM, DCA, and the Legal Division developed FDIC's *Privacy Policy Statement*. This approach was appropriate; in fact, we found it was a recommended approach for developing such a policy. However, during the review, as issues emerged with respect to interpretation of OMB guidance and implementation of FDIC's *Privacy Policy Statement*, there was some degree of confusion among officials in determining the appropriate boundaries of responsibility. Given the current visibility and scrutiny privacy policies are receiving, we believed it was important for the Corporation to have a focal point to address this issue as well as other privacy-related issues that do not fit under the umbrella of the Privacy Act.

In this vein, we believed ongoing changes in technology would cause new issues and new expectations to arise regarding privacy. According to FDIC's *Information Technology Strategic Plan*, FDIC's strategy is to expand the use of the Internet and Intranet for both internal and external communication and transaction processing. Not only are Internet privacy issues emerging daily, but employee privacy issues are also on the rise because of technology. In addition, FDIC must also ensure that privacy issues are considered in the development of new systems, a role now fulfilled in part by the Privacy Act Officer.

Moreover, privacy issues extend beyond the context of the Internet, FDICnet, and systems development at FDIC. As a regulatory agency, FDIC must be sensitive to financial privacy concerns of consumers. Under the newly enacted Gramm-Leach-Bliley Act, FDIC was part of a team of regulators that developed a rule that, in part, will require financial institutions to provide notice to customers about its privacy policies and practices. Going forward, FDIC will be responsible for regulating institutions' implementation of the final rule with regard to privacy policies and practices. We believed FDIC needed to ensure that the implications of this legislation and rule are understood corporate-wide.



The growing impact of privacy concerns on organizations is not unique to FDIC. In the private sector, some of the largest banks are appointing corporate privacy officers. The intent of doing so is to give privacy visibility and send a message that privacy is considered an important area of concern to be addressed. We also learned that some federal agencies, including the Internal Revenue Service and the Department of Health and Human Services, have appointed Privacy Advocates, whose primary responsibility is to oversee their agency's compliance with privacy laws and to participate in the development of privacy policies. In both organizations, these Privacy Advocates are senior level officials distinct from Privacy Act Officers. More specifically, these officials are responsible for such things as:

- consulting on proposals for new data systems, for programs requiring new collections of data, and for regulatory and legislative actions necessitating data collection, and providing advice on the implications of personal privacy;
- conducting or commissioning research and technical studies on disclosure policies;
- focusing on issues of use and disclosure of personal information for other agencies of government, as well as privacy and consumer advocacy organizations, and private-sector organizations that use personal data; and
- training employees on privacy issues and policies, including the seriousness of non-compliance.

Certainly, the concern for privacy is heightened by the nature of the information handled by these agencies. However, we believed the concept of a focal point for privacy, such as these Privacy Advocates, should be studied further by FDIC management. Accordingly, we recommended that:

The Chief Operating Officer, Chief Financial Officer, and General Counsel:

6. Form a working group to study, and prepare a report on, the need for establishing a focal point in the Corporation for privacy issues. This focal point could either be a senior-level official or a committee of senior-level officials that would:
  - promote privacy awareness throughout the Corporation,
  - provide consultation and technical expertise on incorporating privacy principles into data systems and business activities, and
  - be a point of contact and source of information on privacy issues as they relate to the Corporation's bank regulatory oversight responsibilities.

We suggested that the working group consist of representatives of divisions most impacted by privacy issues, regulations, and legislation. The resulting report could be presented to the Operating Committee or Chairman's Working Group, whichever is deemed to be the most appropriate based on the nature of the issue and outcome of the study.

### Corporation Response and OIG Evaluation

We received written responses to our draft report from the General Counsel and Director, DIRM. Specifically, on May 15, 2000, we received a response from the General Counsel addressing recommendations 1 and 6. On May 17, 2000, the Director, DIRM provided a response to recommendations 2 through 5. Overall, both the Legal Division and DIRM agreed with the report's findings and recommendations. The responses provided the requisite elements of a management decision for each of the recommendations. Management's written responses are included in their entirety in Appendix I.


## Corporation Comments



Federal Deposit Insurance Corporation  
550 17th Street NW, Washington, DC 20429

Legal Division

**TO:** Stephen M. Beard, Director  
Office of Congressional Relations and Evaluations  
Office of the Inspector General

**FROM:** William F. Kroener, III   
General Counsel

**SUBJECT:** Response to Draft Evaluation Report: FDIC's Privacy and Security Notices – Requirements and Policy Statements on the Internet and Intranet

The subject draft evaluation report makes six recommendations. This memorandum responds to two of the recommendations, recommendation number one and recommendation number six. The Division of Information Resources Management (DIRM) will respond to recommendations two through five under separate memorandum.

We agree with recommendations one and six and either have already taken action to implement the recommendations or will do so in the near future, as noted below.

### Recommendation 1.

**Recommendation:** FDIC's General Counsel should have FDIC's Office of Executive Secretary complete its review of web pages we identified and add any necessary links to the *Privacy Policy Statement* and any required Privacy Act notices.

**Response:** As recommended, OES has completed its review of web pages that may require a link to the *Privacy Policy Statement* or a Privacy Act notice, including all pages identified by the OIG. As a result of this review, two new Privacy Act notices were added to web pages in January 2000. In another case, OES recommended to the Office of Public Affairs (formerly the Office of Corporate Communications) and to DIRM that an existing Privacy Act notice be made accessible directly from the front page of an on-line form. Finally, OES has also recommended to the Office of Public Affairs and to DIRM that a link to the *Privacy Policy Statement* be added to eleven web pages.

### Recommendation 6.

**Recommendation:** [W]e recommend that the Chief Operating Officer, Chief Financial Officer and General Counsel form a working group to study, and prepare a report on, the need for establishing a focal point in the Corporation for privacy issues. This focal point could either be a senior-level official or a committee of senior level officials that would:

## Corporation Comments

- promote privacy awareness throughout the Corporation,
- provide consultation and technical expertise on incorporating privacy principles into data systems and business activities, and
- be a point of contact and source of information on privacy issues as they relate to the Corporation's bank regulatory oversight responsibilities.

We suggest that the working group consist of representatives of divisions most impacted by privacy issues, regulations and legislation. The resulting report could be presented to the Operating Committee or Chairman's Working Group, whichever is deemed to be the most appropriate based on the nature of the issue and outcome of the study.

**Response:** Representatives of the Legal Division have discussed the recommendation to form a working group to study (and prepare a report on) the need for establishing a focal point in the Corporation for privacy issues with the Executive Secretary (Robert Feldman), the Executive Assistant to the Chief Financial Officer (Gail Verley), and the Special Advisor to the Chief Operating Officer (James Collins). All agree that a study would be beneficial and a group as recommended in the OIG report will be formed no later than June 15, 2000.

Please feel free to contact Linda Rego in the Legal Division or Fredrick Fisch in the Office of the Executive Secretary with any questions regarding this memorandum.

cc: Vijay Deshpande, Director, OICM

## Corporation Comments

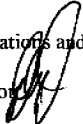


**Federal Deposit Insurance Corporation**  
3501 North Fairfax Dr., Arlington, VA 22226

Division of Information Resources Management

May 17, 2000

**TO:** Stephen M. Beard, Director  
Office of Congressional Relations and Evaluation

**FROM:** Donald C. Demitros, Director 

**SUBJECT:** DIRM Management Response to the Draft OIG Report Entitled, "FDIC's Privacy and Security Notices – Requirements and Policy Statements on the Internet and Intranet" (Audit No. T99-007E)

The Division of Information Resources Management (DIRM) has reviewed the subject draft audit report and generally agrees with the findings and recommendations. DIRM is responding to recommendation numbers 2,3,4 and 5 in this management decision. The Legal Division is responding to recommendation numbers 1 and 6. Responses to each of the OIG's specific recommendations directed to DIRM are provided below:

Recommendation: The Director, DIRM, should have the Chief, Internet Publications Section:

- (2) Contact the CIO Council and review the proposed security notice language and determine how the Corporation will respond to the pending guidance from the CIO Council.

Response: The Internet Publications Section (IPS) has reviewed the CIO Council's proposed security notice language and will implement a security notice on FDIC's Internet web site by June 30, 2000.

- (3) Develop guidance for Internet Coordinators and Webmasters and ensure through training or other means deemed appropriate that they are aware of privacy-related disclosure requirements of OMB Memorandum 99-18 and the Privacy Act. As appropriate, existing procedures for reviewing information posted on FDIC's Internet web site should be modified to reflect guidance developed.

Response: IPS will develop guidance for Internet Coordinators and Webmasters to ensure awareness of privacy-related disclosure requirements of OMB Memo 99-18 and the Privacy Act by November 30, 2000. IPS will modify existing procedures for reviewing information posted on the FDIC's Internet web site to reflect that guidance.

## Corporation Comments

- 2 -

Recommendation: The Director, DIRM should have the Chief, Information Security Staff:

- (4) Develop a notice for FDIC's internal network addressing employee privacy.

Response: The Information Security Section (ISS) will develop the privacy statement in conjunction with the Legal Division and then deliver the statement and requirement to Infrastructure by July 31, 2000.

Once developed, the Director, DIRM should have the Assistant Director, Operations Branch:

- (5) Visibly post the notice developed by the Chief, Information Security Staff on FDIC's internal network.

Response: Infrastructure will implement a pilot to visibly post the privacy statement on FDIC's internal network by September 30, 2000 with full implementation by October 31, 2000.

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

## Appendix II

### 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	The Office of Executive Secretary completed its review of web pages that were identified by the OIG as potentially lacking necessary links to the <i>Privacy Policy Statement</i> and/or Privacy Act notices.	Completed	Memorandum from OES describing results of their review.	No	Yes
2	Division of Information Resources Management (DIRM) Internet Publication Section (IPS) has reviewed the Chief Information Officers Council's proposed security notice and will implement a security notice on FDIC's Internet web site.	06/30/00	Copy of security notice posted on FDIC's Internet web site.	No	Yes
3	IPS will develop guidance for Internet Coordinators and Webmasters to ensure awareness of privacy-related disclosure requirements. In addition, existing procedures for reviewing information posted on FDIC's Internet web site will be modified to reflect the guidance developed.	11/30/00	Guidance issued to Webmasters and Internet Coordinators and modified procedures.	No	Yes

4	DIRM's Information Security Section will develop a privacy statement in conjunction with the Legal Division and provide that statement to DIRM's Technical Infrastructure staff to post on the internal system.	07/31/00	Privacy statement developed by DIRM and Legal Division.	No	Yes
5	DIRM's Technical Infrastructure staff will visibly post the privacy statement on FDIC's internal network after a 1-month pilot implementation.	10/31/00	Copy of privacy notice posted on FDIC's internal network.	No	Yes
6	A working group will be formed to study and prepare a report on the need for establishing a corporate focal point for privacy issues.	06/15/00	Memorandum documenting formation of working group.	No	Yes



### **FDIC's External Web Site *Privacy Policy Statement***

The FDIC is strongly committed to maintaining the privacy of your personal information. The following discloses our information gathering and dissemination practices for this site. The information the FDIC receives depends upon your actions when visiting the Corporation's web site.

#### **Information Collected About Your Visit to the Web Site**

The FDIC automatically collects and stores the following information about you when you visit our Web site:

- The date and time the request was received.
- Your Internet Protocol (IP) address, or the proxy address of your Internet Service Provider (e.g. AOL, CompuServe, and so on).
- The name and IP address of the FDIC server that received and logged the request.
- The resource on an FDIC server accessed as a result of the request, such as the Web page, image, and so on.
- The query in the request. This field captures any criteria or parameters issued with a query, such as a bank name or insurance certificate number.
- The name and version of the your Web browser (e.g. Netscape 4.0).
- The content of any sent or received cookie.
- The Uniform Resource Locator (URL) that was accessed before the user made a request for FDIC's Web server. The URL may be an outside address that is not related to the FDIC server.
- Other status codes and values resulting from the Web server responding to the request received: HTTP status code, Windows NT code, number of bytes sent, number of bytes received, duration (in seconds) to fulfill the request, server port number addressed, and protocol version.

Some parts of the FDIC Web site may use a "cookie", which is a file placed on your computer hard drive, that allows the FDIC web server to log the pages you use in the FDIC site and to determine if you have visited the site before. The cookie captures no personally identifying information. The FDIC server uses this information to provide certain features during your visit to the Web site. You can set your browser to warn you when placement of a cookie is requested, and decide whether or not to accept it. By rejecting a cookie some of the features available on the site may not function properly.

Other than the automatic data collection described above, this site collects no personally identifying information. **The sole exception is when you knowingly and voluntarily provide information**, such as when you fill in your name and address on the FOIA request form.

The FDIC uses the information we collect for internal system administrative purposes to measure the volume of requests for specific web site pages, and to continually improve the FDIC Internet site to be responsive to the needs of users. Your choice to use the FDIC Web site or to send electronic mail to FDIC will be considered your consent for the FDIC to use the information collected therefrom as stated in this notice.

### Information Collected From You

You may decide to send the FDIC information, including personally identifying information. The information you supply – whether through a secure Web form, a standard Web form, or by sending an electronic mail message – is maintained by the FDIC for the purpose of processing your request or inquiry. The FDIC also uses the information you supply in other ways to further the FDIC's mission of maintaining stability and public confidence in the nation's banking system.

Various employees of the FDIC may see the information you submit in the course of their official duties. The information may also be shared by the FDIC with third parties to advance the purpose for which you provide the information, including other federal or state government agencies. For example, if you file a complaint, it may be sent to a financial institution for action, or information may be supplied to the Department of Justice in the event it appears that federal criminal statutes have been violated by an entity you are reporting to the FDIC. The primary use of personally identifying information will be to enable the government to contact you in the event we have questions regarding the information you have reported.

Under certain circumstances, the FDIC may be required by law to disclose information you submit to the Corporation, for example, to respond to a Congressional inquiry or subpoena.

If you register with an FDIC online mailing list, the information you provide may also be used to send you FDIC communiqués or notify you about updates to our web site.

When you choose to send e-mail to the FDIC you are consenting to the FDIC using the information provided therein, including personally identifying information, in accordance with this notice, unless you expressly state in the e-mail your objection to any use(s).

As required by federal law, Privacy Act statements are located throughout this web site where the FDIC requests information from you.

### Contacting the FDIC About This Web Site

If you are concerned about how information about you may have been used in connection with this web site, or you have questions about the FDIC's privacy policy and information practices you should contact:

**FDIC Webmaster**  
**FDIC**  
**550 17th Street, N.W.**  
**Washington, DC 20429**

**E-mail:** [webmaster@fdic.gov](mailto:webmaster@fdic.gov)

Electronic mail is not necessarily secure. You should be very cautious when sending electronic mail containing sensitive, confidential information. As an alternative, you should give consideration to sending it by postal mail.

### **CIO Council's Proposed Security Notice**

This web site is part of a Federal computer system used to accomplish Federal functions. The [Agency name] uses software programs to monitor this web site for security purposes to ensure it remains available to all users and to protect information in the system. By accessing this web site, you are expressly consenting to these monitoring activities.

Unauthorized attempts to defeat or circumvent security features, to use the system for other than intended purposes, to deny service to authorized users, to access, obtain, alter, damage, or destroy information, or otherwise to interfere with the system or its operation is prohibited. Evidence of such acts may be disclosed to law enforcement authorities and result in criminal prosecution under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act of 1996, codified at section 1030 of Title 18 of the United States Code, or other applicable criminal laws.