

June 30, 2006

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum */RA/*
Assistant Inspector General for Audits

SUBJECT: EVALUATION OF PERSONAL PRIVACY
INFORMATION FOUND ON NRC NETWORK
DRIVES (OIG-06-A-14)

This report presents the results of the subject evaluation. Agency comments provided at the exit conference on May 18, 2006, and in a written response, dated June 20, 2006, have been incorporated, as appropriate, into this report. Appendix C contains a copy of the agency's written comments and our response.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG follow up as stated in Management Directive 6.1.

We appreciate the courtesies and cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 301-415-5915, or Beth Serepca at 415-5911.

Attachment: As stated

Electronic Distribution

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
William M. Dean, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Michael R. Johnson, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Janet R. Schlueter, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

EVALUATION REPORT

Evaluation of Personal Privacy Information
Found on NRC Network Drives

OIG-06-A-14 June 30, 2006



All publicly available OIG reports (including this report) are accessible through
NRC's Web site at:

<http://www.nrc.gov/reading-rm/doc-collections/insp-gen/>



**Office of the Inspector General
Personal Privacy Information
Found on NRC Network Drives**

**Contract Number: GS-00F-0001N
Delivery Order Number: DR-36-03-346**

June 29, 2006

[Page intentionally left blank]

TABLE OF CONTENTS

I. BACKGROUND 1

II. FINDING 2

III. RECOMMENDATIONS 6

IV. AGENCY COMMENTS 7

Appendices

A. SCOPE AND METHODOLOGY 9

B. ILLUSTRATION OF INFORMATION FOUND 11

C. FORMAL AGENCY COMMENTS 21

D. DETAILED OIG ANALYSIS OF AGENCY COMMENTS 25

[Page intentionally left blank]

I. BACKGROUND

As a part of the Fiscal Year (FY) 2006 Federal Information Security Management Act (FISMA) independent evaluation of the Nuclear Regulatory Commission's (NRC) information security program, Richard S. Carson and Associates, Inc. (Carson Associates) identified an issue that warrants your attention. Carson Associates found personal privacy information, including Social Security numbers and dates of birth, on NRC network drives that can be accessed by all agency network users. This information may be subject to the provisions of the Privacy Act of 1974.

Personal privacy information was found on NRC network drives that can be accessed by all agency network users because (1) NRC employees are not following existing guidance for protecting personal privacy information, and (2) NRC lacks procedures for monitoring NRC network drives for sensitive data. As a result, NRC employees could be at risk for identity fraud, and the agency may not be in compliance with the Privacy Act.

Personal Privacy Information

Personal privacy information is information about an individual including, but not limited to, Social Security number, home address, home telephone number, date of birth, and financial and medical information.¹ Information in identifiable form is information in an information technology system or online collection: (i) that directly identifies an individual (e.g., name, address, Social Security number or other identifying number or code, telephone number, e-mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.²

The Privacy Act of 1974, as amended (5 U.S.C. § 552a), establishes safeguards for the protection of records the Federal government collects, maintains, uses, and disseminates on individuals. The Privacy Act applies to a specific category of personal privacy information in an identifiable form — records³ retrieved by a personal identifier from an agency system of records.⁴ A personal identifier can be a number assigned to an individual or the individual's Social Security number.

Personal privacy information and information in an identifiable form that is not protected by the Privacy Act also requires appropriate safeguards. Guidance from OMB reminds agencies they are required to inform and educate employees and contractors of their responsibility for protecting information in identifiable form. OMB just recently issued a memorandum on safeguarding personally identifiable information.⁵ That memorandum includes a requirement to

¹ NRC Yellow Announcement 064, "Personal Privacy Information," September 26, 2005.

² Office of Management and Budget (OMB) Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2002.

³ A record is any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

⁴ A system of records is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by an identifying number, symbol, or other identifier assigned to an individual.

⁵ OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information," May 22, 2006.

remind employees of their specific responsibilities for safeguarding personally identifiable information.

II. FINDING

As a part of the FY 2006 FISMA independent evaluation of the NRC's information security program, Carson Associates found personal privacy information, including Social Security numbers and dates of birth, on NRC network drives that can be accessed by all agency network users. This information may be subject to the provisions of the Privacy Act of 1974.

Personal privacy information was found on the NRC network drives because (1) NRC employees are not following existing guidance for protecting personal privacy information, and (2) NRC lacks procedures for monitoring NRC network drives for sensitive data. As a result, NRC employees could be at risk for identity fraud, and the agency may not be in compliance with the Privacy Act.

NRC Network Drives

When an NRC employee logs in to the NRC network, several local and network drives are made available for use. Local drives are those drives found on the employee's local workstation (e.g., the C: drive). Network drives are those drives found on the NRC network and allow the employee to share those drives, and the files stored on them, with other NRC employees. Some network drives have limited access, while others can be accessed by all agency network users.

According to an NRC announcement dated December 10, 2004, the standard NRC workstation local drives are:

- **A: drive** – diskette drive; used for reading/writing diskettes.
- **C: drive** – primary hard disk drive; used for storage of operating system and applications programs and data.
- **D: drive** – Compact Disk Read-Only Memory (CD-ROM) drive; used for reading data from CD-ROMs.

The standard NRC workstation network drives are:

- **G: drive** – network storage location for an organization, usually at the Office level, to share files and documents (referred to as the "Group" drive).
- **P: drive** – network storage location for individual use (referred to as the "Personal" drive).
- **R: drive** – network storage location for viewing, not editing, files, and documents used by multiple organizations (referred to as the "Read-only" drive). The R: drive on each server can be accessed by all agency network users.
- **S: drive** – network storage location for files to be shared among multiple organizations (referred to as the "Shared" drive). The S: drive on each server can be accessed by all agency network users.

- **Y: drive** – network storage location for application-related files shared among multiple organizations. For example, the blank forms used for Informs are stored here. The Y: drive on each server can be accessed by all agency staff; however some files and folders are available for viewing, but not editing.

Carson Associates found the personal privacy information on an R: drive, which according to the NRC announcement, can be accessed by all agency network users.

NRC Employees Are Not Following Existing Guidance

To protect the rights of individuals from invasion of personal privacy, NRC has management controls throughout its policies and procedures regarding the protection of personal privacy information. However, NRC's protection of personal privacy information is weakened by staff failing to follow the agency's established policies and procedures.

Management Directive (MD) and Handbook 3.2, *Privacy Act*, Part V, define the responsibilities of NRC employees who work with records containing information about individuals, including the responsibilities of NRC employees. These responsibilities include:

- Disseminate no information concerning individuals to other NRC employees unless they have a "need to know" the information in order to perform their official duties.
- Maintain and process information concerning individuals in a manner that will ensure no inadvertent or unauthorized disclosures are made of the information.

MD and Handbook 12.5, *NRC Automated Information Security Program*, state that users shall protect sensitive unclassified information in his or her possession from unauthorized access, disclosure, modification, misuse, damage, or theft.

In addition to the policies and procedures described above, the NRC Office of Information Services issues periodic reminders to NRC employees regarding their responsibility to protect personal privacy information. The most recent reminder was sent in the form of a Yellow Announcement to all NRC employees on September 26, 2005. The Yellow Announcement defined personal privacy information as information about an individual, including, but not limited to, Social Security number, home address, home telephone number, date of birth, and financial and medical information. NRC employees and contractors were reminded of their responsibility to protect personal privacy information, whether the information is their own or about others.

In addition, the NRC announcement regarding NRC local and network drives, dated December 10, 2004, specifically reminded staff that when a file or document is saved, staff should be aware of the location where the data is being stored. The announcement also reminded staff that files on an R: drive can be viewed by other network users and that data that needs protection from access by other network users can be placed on a diskette or other removable storage media and appropriately stored away from the workstation.

Despite NRC's policies and procedures regarding the protection of personal privacy information and the periodic reminders sent by the Office of Information Services, Carson Associates found several documents containing personal privacy information, including Social Security numbers and data of birth, on NRC network drives that can be accessed by all agency network users. Some of these files include:

- Excel spreadsheets including bonus awards information for Senior Executive Service personnel (including Social Security numbers)
- Excel spreadsheet containing over 500 employee names and Social Security numbers
- Eight text files, each containing over 500 employee names, Social Security numbers, and dates of birth

According to the agency, R: drives are read only for users. Files are added to it by systems administrators in the Network Operations Center who have write privileges. See Appendix B for screen shots of some of the files found on the NRC network drives. NOTE: Appendix B will be redacted in the publicly available version of the report.

NRC Lacks Procedures for Monitoring NRC Network Drives

MD and Handbook 3.2 state that office directors and regional administrators are responsible for conducting periodic reviews of systems of records under their control to ensure compliance with guidelines and procedures implementing the Privacy Act.

However, none of NRC's policies and procedures specifically describe procedures for monitoring NRC network drives for the presence of personal privacy information to ensure it is being properly controlled in accordance with the NRC policies and procedures. According to the agency, drive owners frequently review shared drive components, however only on an ad hoc basis.

These ad hoc reviews are not sufficient, as some of the files found containing personal privacy information are almost 10 years old.

NRC Employees Are At Risk for Identity Fraud

Due to the presence of personal privacy information on NRC network drives that can be accessed by all agency network users, NRC employees are at risk for identity fraud. Identity fraud is the deliberate assumption of another person's identity, most often to gain access to his or her finances. Approximately 11.8 million Americans (1 in 20 adults) have been victimized by identity fraud as of April 2003, according to research by Star Systems. In many instances, a criminal only needs a name, Social Security number, and date of birth to commit identity fraud. Identity fraud can result in both financial costs to the victim, but also lost time spent trying to restore damaged credit resulting from the identity fraud.

The Agency May Not Be In Compliance With the Privacy Act

The personal privacy information found on NRC network drives that can be accessed by all agency network users is similar to information found in more than one of NRC's systems of records published in the *Federal Register*⁶ and also fits the definition of a *duplicate system of records*. As defined in MD and Handbook 3.2, a duplicate system of records is a group of records that are similar to records contained in an NRC system of records. It need not contain all of the records contained in the primary system. The information also meets the criteria of a "record" as defined by the Privacy Act.

Carson Associates could not determine whether the personal privacy information found on the NRC network drives came from, or is maintained as a part of, a Privacy Act system of records, or if the information is considered a duplicate system of records. However, if the information did come from a system of records, or is determined to be a duplicate system of records, then the agency may not be in compliance with the Privacy Act.

⁶ Federal agencies covered by the Privacy Act are required to publish descriptions of their systems of records in the *Federal Register*. Each *Federal Register* notice for a system of records includes information regarding agencies policies and practices regarding storage, retrieval, safeguards, and disposal of records in the system.

III. RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Remind employees of their responsibilities to protect personal privacy information.
2. Remind employees that files on network drives may be viewed by other network users and that personal privacy information should not be posted on network drives unless access to that information is appropriately restricted to users with a “need to know.”
3. Develop policies and procedures for reviewing network drives for the presence of personal privacy information.
4. Conduct an immediate review of all network drives for the presence of personal privacy information and remove any information that should not be posted on a network drive unless access to that information is appropriately restricted to users with a “need to know.”

IV. AGENCY COMMENTS

At an exit conference with the agency held on May 18, 2006, the agency provided informal comments and generally agreed with the report recommendations. On June 20, 2006, the agency provided a formal response with additional comments. Where appropriate, the Office of the Inspector General (OIG) modified the report in response to these comments. Appendix C contains a copy of the agency's formal written comments. Appendix D contains OIG's specific responses to the agency's comments.

[Page intentionally left blank]

A. SCOPE AND METHODOLOGY

To prepare this report, Carson Associates reviewed MD 3.2 and MD 12.5, NRC's Privacy Act systems of records notice in the *Federal Register*, and several NRC announcements found on the NRC internal web site. Carson Associates also conducted an interview with NRC's senior information technology security officer and other staff members from the Office of Information Services. The work was conducted during April and May 2006 in accordance with best practices for evaluating security controls. Jane M. Laroussi, CISSP, and Kelby M. Funn, CISA, from Carson Associates conducted the work.

[Page intentionally left blank]

B. ILLUSTRATION OF INFORMATION FOUND

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY APPENDIX HAS BEEN REDACTED FOR PUBLIC RELEASE

[Page intentionally left blank]

C. FORMAL AGENCY COMMENTS

From: Melinda Malloy
To: Beth Serepca
CC: Paulette Bosco, Catherine Holzle, William Dean, Vicki Foster, Edward Baker, Margie Janney, Jane Laroussi, Russell Nichols, Sandra Northern, John Linehan, Brenda Shelton, Karen Olive
Date: Wednesday - June 28, 2006
Subject: OUO markings on comment memo re: final draft audit report

Beth,

The staff provided written comments on OIG's final draft audit report, Personal Privacy Information Found on NRC Network Drives, in a memo from Luis Reyes, EDO to Steve Dingbaum dated June 20, 2006. This document was marked "Official Use Only - Sensitive Internal Information" due to the markings on the draft OIG audit report. OEDO and OIS have reviewed the memo and have no objection to its inclusion in OIG's final audit report. To facilitate completion of the audit report, you may strike out the markings, top & bottom, on all pages of the memo and annotate the first page to reflect our agreement to put the memo in the final audit report. I will have OIS correct the official record copy of the memo.

Melinda Malloy, OEDO
OIG Audit Liaison
415-1785

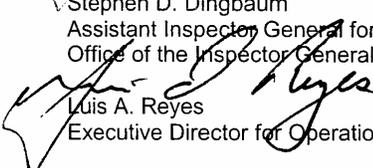


~~Official Use Only - Sensitive Internal Information~~

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

June 20, 2006

MEMORANDUM TO: ✓ Stephen D. Dingbaum
Assistant Inspector General for Audits
Office of the Inspector General

FROM: 
Luis A. Reyes
Executive Director for Operations

SUBJECT: COMMENTS ON DRAFT AUDIT REPORT: PERSONAL
PRIVACY INFORMATION FOUND ON NRC NETWORK DRIVES

In response to your memorandum of June 1, 2006, I am providing comments on the Office of the Inspector General (OIG) Draft Audit Report "Personal Privacy Information Found on NRC Network Drives." The staff appreciates that the OIG revised the report to accommodate some of the comments which the staff provided and discussed during the May 18, 2006, exit conference. However, the staff remains concerned that the report continues to emphasize Privacy Act considerations, as demonstrated by the centrality of that statute and related guidance in the body of the report. Therefore, I have enclosed additional comments on the draft report for your consideration.

Enclosure:
As stated

Official Use Only Marking Removed Per
OEDO E-mail Dated 6/28/06 - See Page 21

~~Official Use Only - Sensitive Internal Information~~

~~Official Use Only - Sensitive Internal Information~~

OFFICIAL RECORD COPY
COMMENTS ON THE
OIG REVISED DRAFT AUDIT REPORT ON PERSONAL
PRIVACY INFORMATION FOUND ON NRC NETWORK DRIVES

- General Document Text
 - Throughout the document the phrase “accessed by all agency network users” should be revised to read “accessed by agency network users assigned to the particular server.” The statement, as currently written in the report, exaggerates the size of the population that had potential access to the information.
 - The Privacy Act of 1974 is referred to in this document as the “Federal” Privacy Act of 1974. The word “Federal” is not part of the proper name of the statute and should be removed.
 - Reference to Management Directive 3.2, “Privacy Act,” is inappropriate, since it presumes that the Privacy Act is a core issue in this matter. The reference to the Privacy Act is emphasized in the report and creates the mistaken impression that some kind of Privacy Act violation was found.
- Background
 - The second paragraph provides the correct definitions of a record and a system of records under the Privacy Act. However, it is important to note that the described types of records would be protected by the provisions of the Privacy Act only if they were part of a system of records. These types of records can exist in a collection or grouping of agency records that do not meet the criteria for a system of records (where information is not retrieved by a name or personal identifier) and therefore would not be protected by the Privacy Act.
- Findings
 - NRC Employees Are Not Following Existing Guidance, pages 3-5
 - The end of the first sentence in the first paragraph reads “ensure that personal privacy information is protected from unauthorized disclosure” and implies two things that are incorrect. One is that the agency made an affirmative release of the information (implied from use of the term “disclosure” versus “permitting access” or something similar). The other is the suggestion that there is a Privacy Act violation, due to reliance on the term “unauthorized.” This overstates the situation. The phrase “unauthorized disclosure” should be replaced with “uncontrolled access.” The availability of personal privacy information on the network drives is not an unauthorized disclosure but a failure by the staff to institute appropriate access controls.

Enclosure

~~Official Use Only - Sensitive Internal Information~~

~~Official Use Only - Sensitive Internal Information~~

2

- Regarding the last sentence of the last paragraph, in the event the final document is released to the public, the public version should not include the enclosure referenced in the document. The enclosure contains actual samples of some of the personal privacy information, and that release itself would result in a much greater breach of an individual's expectation of privacy than that highlighted in the report.
- NRC Employees Are At Risk For Identity Fraud, page 6
 - The section heading and first sentence imply that there remains a threat of identity theft. The staff took immediate action and deleted the files identified in the report that contained personal privacy information. Therefore, the sentence should clarify this point along the following lines: "The presence of personal privacy information on NRC network drives that can be accessed by agency network users may place NRC employees at risk for identity fraud." A more accurate heading for this section would be "Risk of Identity Fraud."
- The Agency May Not Be In Compliance With The Privacy Act, page 6
 - There is no basis upon which to make this assertion, since it has not been established that any Privacy Act information was involved in this matter, as acknowledged in the report itself. Therefore, there is far too much emphasis on the Privacy Act, including reference to the definition of a "duplicate system of records," which is specific to the Privacy Act. Taken together, the clear implication is that a Privacy Act violation occurred, but the plain evidence of that is lacking. Misplaced reference to the Privacy Act in the report as a whole repeatedly hints that violations of this law occurred, which has no foundation in fact.
- Recommendations, page 7
 - The recommendations could acknowledge that the agency already takes action as described in at least one recommendation; namely, the agency does remind employees of their responsibilities to protect personal privacy information. Indeed, in the section entitled "NRC Employees Are Not Following Existing Guidance," the report credits the Office of Information Services with issuing "periodic reminders to NRC employees regarding their responsibility to protect personal privacy information," and the report even refers to the most recent reminder in the form of a Yellow Announcement dated September 26, 2005.

~~Official Use Only - Sensitive Internal Information~~

D. DETAILED OIG ANALYSIS OF AGENCY COMMENTS

At an exit conference with the agency held on May 18, 2006, the agency provided informal comments and generally agreed with the report recommendations. On June 20, 2006, the agency provided a formal response with additional comments (see Appendix C).

Below is OIG's analysis of the agency's formal comments. NRC's comments appear in bold italics.

Throughout the document the phrase "accessed by all agency network users" should be revised to read "accessed by agency network users assigned to the particular server." The statement, as currently written in the report, exaggerates the size of the population that had potential access to the information.

OIG did not modify the report. According to the NRC announcement dated December 10, 2004, the "R: drive on each server can be accessed by all agency network users." The personal privacy information was found on an "R:" drive; therefore according to the announcement, it can be accessed by all agency network users. Further, the agency was unable to provide support that the drive is restricted.

The Privacy Act of 1974 is referred to in this document as the "Federal" Privacy Act of 1974. The word "Federal" is not part of the proper name of the statute and should be removed.

OIG modified the text as recommended. However it should be noted that MD 3.2 and the accompanying Handbook include the word "Federal" when introducing the Act for the first time.

Reference to Management Directive 3.2, "Privacy Act," is inappropriate, since it presumes that the Privacy Act is a core issue in this matter. The reference to the Privacy Act is emphasized in the report and creates the mistaken impression that some kind of Privacy Act violation was found.

OIG did not remove references to MD 3.2, as this directive was used to determine whether the Privacy Act was applicable to the information found on the NRC network drives. One of the objectives of the directive is to "ensure that NRC collects, maintains, uses, and disseminates any record of identifiable personal information in a manner that ensures that the action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of the information."

The second paragraph provides the correct definitions of a record and a system of records under the Privacy Act. However, it is important to note that the described types of records would be protected by the provisions of the Privacy Act only if they were part of a system of records. These types of records can exist in a collection or grouping of agency records that do not meet the criteria of a system of records (where information is not retrieved by a name or personal identifier) and therefore would not be protected by the Privacy Act.

OIG modified the text to include the definitions of personal privacy information and information in an identifiable form, which also require adequate safeguards. The definitions of a record and a system of records remain in the report, but as footnotes. However, it should be noted that some courts have held that the “system of records” threshold requirement is not necessarily applicable to all subsections of the Act, including the subsection requiring the establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.⁷ Some courts have held that this subsection can also apply to records that are not part of a system of records.

NRC Employees Are Not Following Existing Guidance, pages 3-5 (which appears on pages 3-4 of this final report)

The end of the first sentence in the first paragraph reads “ensure that personal privacy information is protected from unauthorized disclosure” and implies two things that are incorrect. One is that the agency made an affirmative release of the information (implied from the use of the term “disclosure” versus “permitting access” or something similar). The other is the suggestion that there is a Privacy Act violation, due to reliance on the term “unauthorized.” This overstates the situation. The phrase “unauthorized disclosure” should be replaced with “uncontrolled access.” The availability of personal privacy information on the network drive is not an unauthorized disclosure but a failure by the staff to institute appropriate access controls.

OIG modified the text to describe the agency’s policies and procedures as being related to the protection of personal privacy information rather than unauthorized disclosure.

Regarding the last sentence of the last paragraph, in the event the final document is released to the public, the public version should not include the enclosure referenced in the document. The enclosure contains actual samples of some of the personal privacy information, and that release itself would result in a much greater breach of an individual’s expectation of privacy than that highlighted in the report.

OIG modified the report so that Appendix B, which contains the samples of the personal privacy information, is marked “Official Use Only – Sensitive Internal Information.” Appendix B will be redacted in the publicly available version of the report.

NRC Employees are At Risk for Identity Fraud, page 6 (which appears on page 4 of this final report)

The section heading and first sentence imply that there remains a threat of identity theft. The staff took immediate action and deleted the files identified in the report that contained personal privacy information. Therefore, the sentence should clarify this point along the following lines: “The presence of personal privacy information on NRC network drives that can be accessed by agency network users may place NRC employees at risk for identity fraud.” A more accurate heading for this section would be “Risk of Identity Fraud.”

⁷ “Overview of the Privacy Act of 1974,” United States Department of Justice, May 2004.

OIG did not modify the report as the threat still remains. At least one of the files identified in the report was still on the NRC network drive as of June 28, 2006. The files that have been removed could have been accessed at any time prior to their removal, and the information from those files still could be used to commit identity fraud.

The Agency May Not Be In Compliance With The Privacy Act, page 6 (which appears on page 5 of this final report)

There is no basis upon which to make this assertion, since it has not been established that any Privacy Act information was involved in this matter, as acknowledged in the report itself. Therefore, there is far too much emphasis on the Privacy Act, including reference to the definition of a “duplicate system of records,” which is specific to the Privacy Act. Taken together, the clear implication is that a Privacy Act violation occurred, but the plain evidence of that is lacking. Misplaced reference to the Privacy Act in the report as a whole repeatedly hints that violations of this law occurred, which has no foundation in fact.

OIG did not modify the report. The intent of the report was to alert the agency to the presence of the personal privacy information on NRC network drives, not to investigate where the information came from. The finding only points out that the information found may be Privacy Act information.

Recommendations, page 7 (which appear on page 6 of this final report)

The recommendations could acknowledge that the agency already takes action as described in at least one recommendation; namely, the agency does remind employees of their responsibility to protect personal privacy information. Indeed, in the section entitled “NRC Employees Are Not Following Existing Guidance,” the report credits the Office of Information Services with issuing “periodic reminders to NRC employees regarding their responsibility to protect personal privacy information,” and the report even refers to the most recent reminder in the form of a Yellow Announcement dated September 26, 2005.

OIG did not modify the report. At the exit conference, the agency generally agreed with the report recommendations. The report already acknowledges actions currently taken by the agency. The finding points out that the current actions are not adequate as employees are not following the existing guidance.

[Page intentionally left blank]