September 18, 2002

MEMORANDUM TO: William D. Travers
Executive Director for Operations

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

SUBJECT: MEMORANDUM REPORT: REVIEW OF NRC'S PROTECTION OF SOCIAL SECURITY NUMBERS (OIG-02-A-16)

The Office of the Inspector General (OIG) has completed a review of the agency's controls over the access, disclosure, and use of Social Security Numbers (SSNs) by third parties. This review disclosed a lack of full adherence to agency policy covering this area. Specifically,

- Required clauses to protect SSNs accessed by contractors were not included in all applicable contracts;
- Not all agency systems of records had been included in the *Privacy Act* records; and,
- The controls over duplicate systems of records need to be strengthened.

At an exit meeting on September 5, 2002, agency officials provided comments which have been incorporated into this report, where appropriate.

BACKGROUND

Since the creation of the SSN, the number of Federal agencies and other entities that rely on it has grown beyond the original intended purpose. In 1936, the Social Security Administration created a numbering system designed to provide a unique identifier, the SSN, for each individual. The Social Security Administration uses SSNs to track workers' earnings and eligibility for Social Security benefits, and as of December 1998, 391 million SSNs have been issued. Over the years, the SSN has become a "de facto" national identifier. Because SSNs are unique identifiers, the numbers provide an efficient way to manage records. The expanded use of the SSN provides a tempting motive for many unscrupulous individuals to acquire someone else's SSN and use it for illegal purposes.

No single Federal law regulates the overall use or restricts the disclosure of SSNs by government agencies; however, a number of laws limit SSN use in specific instances. Generally, the Federal government's overall use and disclosure of SSNs are restricted under the *Freedom of Information Act* and the *Privacy Act*. The *Freedom of Information Act* presumes Federal government records are available upon formal request, but exempts certain personal information, such as SSNs.

The purpose of the *Privacy Act* is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against invasions of their privacy stemming from Federal agencies' collection, maintenance, use and disclosure of personal information about them. Specifically, with regard to collecting SSNs, Section 7 of the *Privacy Act* prohibits any Federal, State or local agency from denying an individual any right, benefit, or privilege, provided by law because of the individual's refusal to disclose his social security account number. Section 7 of the *Privacy Act* also requires any agency which requests an individual to disclose his/her SSN to inform the individual as to whether the disclosure is mandatory or voluntary, by what statutory authority or other authority the request is made, and how the agency will use the number.

PURPOSE

The Chairman of the House Ways and Means Subcommittee on Social Security requested the President's Council on Integrity and Efficiency[1] to examine the control over SSNs by Federal agencies. The objective of this audit was to assess NRC's controls over the access, disclosure, and use of SSNs by third parties. Specifically, OIG determined whether NRC:

- Makes legal and informed disclosure of SSNs to third parties;
- Has appropriate controls over contractors' access and use of SSNs;
- Has appropriate controls over other entities' access and use of SSNs; and,
- Has adequate controls over access to individuals' SSNs maintained in its databases.

[1]The President's Council on Integrity and Efficiency (PCIE), comprised primarily of Presidentially appointed Inspectors General (IG), accomplishes its mission by conducting interagency and inter-entity audit, inspection, and investigation projects to promote economy and efficiency in Federal programs and operations and address more effectively government-wide issues of fraud, waste, and abuse. The Council members also develop policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled IG workforce.

RESULTS

To protect the rights of individuals from invasion of personal privacy, NRC has management controls through its policies and procedures to ensure that systems of records[2] are established and maintained. However, NRC's protection of personal information is weakened by staff failing to follow the agency established policies and procedures. Specifically, *Privacy Act* clauses are not always included in applicable contracts, not all applicable NRC records systems are included in *Privacy Act* systems of records[3], and the controls over duplicate systems of records need to be strengthened.

Privacy Act Clause Not Included In Contracts

System managers and project officers were unaware that they needed to inform the Division of Contracts (DC) when their contractors would work on a system of records. As a result, some NRC contracts did not contain the required clauses limiting disclosure of personal information. Without the clauses, the provisions of the *Privacy Act* are not binding on the contractor. *NRC Management Directive 3.2, Privacy Act* requires Office Directors and Regional Administrators to provide adequate safeguards for *Privacy Act* records under their control. In addition, DC is required to ensure that contracts contain the appropriate clauses when the contract provides for contractors' access to and use of an NRC system of records. To make the provisions of the *Privacy Act* binding on the contractor, and his or her employees, *Federal Acquisition Regulation 52.224-1, Privacy Act Notification* and *Federal Acquisition Regulation 52.224-2, Privacy Act* clauses must be referenced in the contract.

In August 2001, the Privacy Program Officer, Office of the Chief Information Officer, conducted a review of 11 randomly selected agency contracts which provide for the maintenance of a system of records. This review is required every two years by the Office of Management and Budget to ensure that the wording of each contract makes the provisions of the *Privacy Act* binding on the contractors and his or her employees. Only 1 of the 11 contracts contained the required clauses. As a result of this review, DC modified the contracts, as necessary, to include the clauses and reminded its staff of the requirement for including *Privacy Act* clauses in contracts. During the conduct of this audit, OIG tested two contracts of these 11 and determined that the clauses had been added.

Subsequently, OIG reviewed 10 contracts, including two previously reviewed by the Privacy Program Officer, involving systems of records, and found 2 contracts that did not include *Privacy Act* clauses. The required Federal Acquisition Regulation clauses

[2] A system of records is a group of *Privacy Act* records under the control of NRC from which information is retrieved by the name of an individual or by an identifying number.

[3] The Federal *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 and applies when information is retrieved by personal identifier. A personal identifier can be a number assigned to an individual or the individual's social security number.

were absent because staff were unfamiliar with the *Privacy Act* requirements. System managers and project officers were unaware that they needed to indicate to DC that the contractor would work on a system of records. Consequently, without the system manager's or project officer's indication, DC contract officers did not recognize the requirement for such a clause.

Systems Not Included In *Privacy Act* Systems of Records

Some NRC systems meet the criteria for *Privacy Act* systems of records, but have not been identified as such. The programmers who developed systems were unaware that the systems should be declared *Privacy Act* records and, therefore, did not inform the Privacy Program Officer of the systems' existence. As a result, NRC has not complied with provisions of the *Privacy Act* which provides individuals with protection from invasion of personal privacy.

According to the *Privacy Act*, any group of records under the control of an agency, where information is retrieved by name or SSN, is a system of records. NRC offices develop and maintain systems where the information contained in the systems are retrieved by name or SSN. However, one system has not been included in the NRC systems of records, and others have not been considered for inclusion in the republication of systems of records in the *Federal Register.*[4] OIG identified 10 systems developed in offices where information is retrieved by an individual's name or SSN that had not been included in the draft republication. For example, one office developed a system to track travel arrangements which contains information retrieved by name or SSN, but is not included among the systems of records. There may be other systems, not reviewed by OIG, that should be treated as systems of records.

Management Directive 3.2, Privacy Act describes the organizational responsibilities and delegations of authority to implement the *Privacy Act*. The directive requires Office Directors and Regional Administrators to obtain advice and assistance from the Privacy Program Officer, as needed, when developing new systems of records or revising existing systems of records to carry out the functions of their offices. It also requires the Privacy Program Officer to periodically review activities involving systems of records to ascertain the level of compliance with the *Privacy Act*.

System programmers were unaware that their systems should be declared systems of records, therefore, they did not notify the Privacy Program Officer. In some situations, the applications were developed to aid the office with administrative record keeping such as training and office equipment tracking. Furthermore, the directive does not provide specific guidance on the process to be used by the Privacy Program Officer to determine whether NRC's offices have systems that have not been declared systems of records. The Privacy Program Officer did not contact individual offices to assess whether their systems meet the criteria for systems of records. OIG examined systems

[4] *OMB Circular A-130, Appendix I* requires agencies to republish descriptions of their systems of records in the *Federal Register*.

at some NRC offices and found systems that met the criteria, but had not been identified as systems of records.

Without identifying all systems of records, NRC is not in compliance with the *Privacy Act* requirements to publish systems of records in the *Federal Register*. The *Privacy Act* states that offenders are subject to criminal penalties and fines up to $5,000 for any officer or employee of the agency who willfully maintains a system of records without first publishing a system notice in the *Federal Register*. In addition, in the event of a *Privacy Act* civil lawsuit, the agency, not the contractor, is liable. While OIG did not identify willful violations of the *Privacy Act* requirements, the penalties emphasize the importance of complying with the *Privacy Act*.

Controls Over Duplicate Systems of Records

The controls over duplicate systems of records need to be strengthened. A duplicate system of records is a group of records that are similar to those contained in a primary system of records. Duplicate systems of records should be maintained the same way as the primary systems of records. *Management Directive 3.2, Privacy Act* requires that the locations of duplicate systems of records be identified in the *Federal Register* notice and that system managers maintain records on duplicate systems of records. This review disclosed that the *Federal Register* notice only provides limited information about NRC's duplicate systems of records. NRC management cannot provide a comprehensive list of duplicate systems of records. The absence of these controls weakens the protection of personally identifiable information contained in duplicate systems of records.

Neither system managers, nor the Privacy Program Officer could provide documentation that:

- All duplicate systems of records have been identified; and,

- Policies and practices regarding storage, retrieval, safeguards and retention, and disposal for the duplicate system of records are the same as for the primary system of records listed in the *Federal Register* notice.

Furthermore, the Privacy Program Officer could not provide documentation that a master list of all duplicate systems of records is maintained.

Sufficient information about duplicate systems of records is not identified in the *Federal Register* notice. Guidance does not require that names of duplicate systems of records be published. Currently, the information about duplicate systems of records identified in the *Federal Register* notice is limited to the indication that the duplicate exists at any one of several NRC street locations. System managers should maintain records of the names, descriptions and office locations of duplicate systems of records. A comprehensive list of duplicate systems of records will enhance NRC's ability to ensure that adequate protections are afforded over duplicate systems of records. It will also provide systems managers with a resource to compare the attributes of the

duplicate systems of records with those of the primary systems of records. Such a comparison will ensure that system managers exercise measures to protect personally identifiable information contained in duplicate systems of record.

CONCLUSION

Agency employees do not consistently follow NRC policy and the policy should be strengthened. NRC's protection of personal information is weakened by staff failing to follow the established policy and procedure. Specifically, *Privacy Act* clauses are not always included in applicable contracts, not all systems of records are included in *Privacy Act* records and the controls over duplicate systems of records need to be strengthened.

RECOMMENDATIONS

We recommend that the Executive Director for Operations:

1. Implement a process for system managers and project officers to inform the Division of Contracts when their contract requirements involve contractor access to NRC systems of records so that *Privacy Act* Clauses are included.

2. Implement measures to enforce established policy regarding system manager and project officer responsibilities to inform the Privacy Program Officer of systems of records and duplicate systems of records.

3. Perform biennial review of NRC offices to determine if all systems of records and duplicate systems of records have been identified.

4. Develop and maintain a comprehensive list of duplicate systems of records under the *Privacy Act*, including all names, descriptions and office locations of these records.

Please provide information on actions taken or planned on each of the recommendations directed to your office by November 1, 2002. Actions taken or planned are subject to OIG follow up.

SCOPE/CONTRIBUTORS

To accomplish the audit objectives, OIG assessed the controls related to the NRC's protection of social security numbers through a questionnaire provided by the President's Council on Integrity and Efficiency. The scope was limited to the objectives requested by the President's Council on Integrity and Efficiency questionnaire. OIG conducted interviews in NRC headquarters and regional offices and observed system demonstrations in regional offices. This work was conducted from January 2002 through July 2002, in accordance with generally accepted Government auditing standards by Ren Kelley, Beth Serepca, and Vicki Foster.

If you have any questions or concerns regarding this memorandum, please contact Ren Kelley, Team Leader, at 415-5977, or me at 415-5915.

cc: J. Craig, OEDO

R. McOsker, OCM/RAM
B. Torres, ACMUI
G. Hornberger, ACNW
G. Apostolakis, ACRS
J. Larkins, ACRS/ACNW
P. Bollwerk III, ASLBP
K. Cyr, OGC
J. Cordes, OCAA
S. Reiter, CIO
J. Funches, CFO
P. Rabideau, Deputy CFO
J. Dunn Lee, OIP
D. Rathbun, OCA
W. Beecher, OPA
A. Vietti-Cook, SECY
W. Kane, DEDR/OEDO
C. Paperiello, DEDMRS/OEDO
P. Norry, DEDM/OEDO
M. Springer, ADM
R. Borchardt, NRR
G. Caputo, OI
P. Bird, HR
I. Little, SBCR
M. Virgilio, NMSS
S. Collins, NRR
A. Thadani, RES
P. Lohaus, STP
F. Congel, OE
M. Federline, NMSS
R. Zimmerman, NSIR
J. Johnson, NRR
H. Miller, RI
L. Reyes, RII
J. Dyer, RIII
E. Merschoff, RIV
OPA-RI
OPA-RII
OPA-RIII
OPA-RIV