Department of Energy
Washington, DC 20585

August 7, 2006

MEMORANDUM FOR: ASSOCIATE DIRECTORS
OFFICE DIRECTORS
SITE OFFICE MANAGERS

FROM: GEORGE MALOSH
ACTING CHIEF OPERATING OFFICER
OFFICE OF SCIENCE

SUBJECT: Office of Science Policy on the Protection of Personally Identifiable Information

The attached Office of Science (SC) Personally Identifiable Information (PII) Policy is effective immediately. This supersedes my July 14, 2006, memorandum providing interim direction on SC implementation of Departmental guidance issued by the Department of Energy Chief Information Officer (CIO). All SC Associate Directors, Office Directors, and Site Office Managers must ensure the prompt implementation and institutionalization of the policy requirements for SC Federal organizations and contractors.

I request that you ensure that all of your staff is notified. It is each employee's responsibility to assess and determine whether or not the information they use is considered PII. If you or any of your staff need assistance in identifying PII or interpreting this direction, please contact the responsible SC CIO or the SC Senior Information Management Executive (SIME). Your support and assistance in this critical effort is greatly appreciated.

All questions should be forwarded to Kimberly Rasar (Acting Senior Information Management Executive) and Mike Robertson (SC Cyber Security Program Manager).

Attachment

DISTRIBUTION LIST

ASSOCIATE DIRECTORS:

Michael Strayer, SC-21
Pat Dehmer, SC-22
David Thomassen, SC-23
Robin Staffin, SC-25
Dennis Kovar, SC-26
Peter Faletra, SC-27

OFFICE DIRECTORS:

Peter Lincoln, SC-1.1
Ralph De Lorenzo, SC-1.21
Bill Valdez, SC-1.22
Daniel Lehman, SC1.3
John LaBarge, SC-31.3
John Alleva, SC-32
Kimberly Rasar, SC-33

FIELD OFFICE MANAGERS:

John Adachi, AMSO
Creig Zook, ASO
Aundra Richards, BSO
Mike Holland, BHSO
Joanna Livengood, FSO
Paul Kruger, PNSO
Jerry Faul, PSO
Nancy Sanchez, SSO
James Turi, TJSO
Bob Wunderlich, CH
Gerald Boyd, OR

SUBJECT: OFFICE OF SCIENCE PERSONALLY IDENTIFIABLE INFORMATION (PII) POLICY

Purpose

The purpose of this document is to establish a high-level Office of Science (SC) protection policy for Personally Identifiable Information (PII) consistent with DOE CIO-Guidance CS-38.

The mission of the Department of Energy's Office of Science is to deliver the remarkable discoveries and scientific tools that transform our understanding of energy and matter and advance the national, economic, and energy security of the United States. This mission relies on open and collaborative communication. DOE information and information systems are appropriately protected to ensure mission success.

Definition of PII

PII: Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security numbers, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Classes of PII

SC has identified two types of PII as follows:

- **Public PII**

  PII is available in public sources such as telephone books, public websites, business cards, university listings, etc. This PII includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. This category of PII will be referred to as Public PII and must be protected with at least NIST SP 800-53 low level controls.

- **Protected PII**

  SC also recognizes there is another category of PII that requires enhanced protection, which will be referred to as Protected PII. This typically includes information which, if compromised, can cause serious or severe harm to an individual (such as identity theft). Protected PII is defined as:

  An individual's first name or first initial and last name in combination with any one or more of the following data elements types of information including, but not limited to, social security number, passport number, credit card numbers,

clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts, etc. requires enhanced protection.

Protected PII must be protected with at least NIST SP 800-53 moderate level controls. When Public PII is combined with Protected PII, then the combined information must also be protected with at least NIST SP 800-53 moderate level controls.

Policy

- **General**

  All electronic copies of Protected PII will reside within an accreditation boundary protected at least at the moderate level. Protected PII is not to be downloaded to mobile devices (such as laptops, Personal Digital Assistants (PDAs), or removable media) or to systems outside the protection of the accreditation boundary.

- **Waiver**

  If there is an operational or business need to store Protected PII outside the accreditation boundary (in particular on laptops and mobile devices), a waiver may be granted by the Designated Approval Authority (DAA). In instances where a waiver has been granted, the controls as specified by DOE CIO CS-38 will be applied. In particular, encryption (FIPS 140-2 compliant) will be used to protect PII and a 90-day review policy will be enforced.

- **Remote Access**

  If there is an operational or business need to access Protected PII data from outside the accreditation boundary an automatic disconnect after 30 minutes of inactivity will be enforced. In addition, 2-factor authentication will be required to access Protected PII.

- **Incident Reporting**

  Within 45 minutes after discovery of a real or suspected loss of Protected PII data, Computer Incident Advisory Capability (CIAC) needs to be notified (ciac@ciac.org). Reporting of incidents involving Public PII will be in accordance with normal incident reporting procedures.

References:

U.S. Public Laws

Privacy Act of 1974 - This Act (Public Law 93-579, as amended, Title 5 U.S. Code section 552a) prohibits disclosure of information in personal records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. Federal Managers' Financial Integrity Act of 1982 (FMFIA) - This Act (Public Law 97-255) provides requirements for executive agency accounting and other financial management reports and plans, including identification and reporting of material weaknesses (section 2, (d)(4)).

Electronic Communications Privacy Act of 1986 - This Act (Public Law 99-508) amends Title 18, United States Code, Chapter 119 with respect to the interception of certain communications, other forms of surveillance, and for other purposes. It also prohibits unauthorized access to an electronic communications system in order to obtain or alter information contained in such system and prohibits the installation or use of a pen register or tracking device without a court order.

Computer Security Act of 1987 (Summary) - In this Act (Public Law 100-235), the Congress declares that improving the security and privacy of sensitive information in Federal computer systems was in the public interest, and created a means for establishing minimum acceptable security practices for such systems.

Federal Information Security Management Act (FISMA, enacted December 2002) - This Act (Title III of the E-Government Act of 2002) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

Office of Management and Budget (OMB) Circular A-11, *Planning, Budgeting, Acquisition of Capital Assets, Strategic Plans, Performance Plans* - This Circular provides guidance on the FY 2004 Budget submission. It also includes instructions on budget execution, integrating agencies' budget and accounting functions, and improving the quality of financial information in accordance with the Government Performance and Results Act of 1993 and other laws. The Circular describes specific steps that agencies must take to integrate budget and performance, a key part of the President's Management Agenda.

OMB Circular A-127, *Financial Management Systems* - This Circular prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems in accordance with the Federal Managers' Financial Integrity Act of 1982 (FMFIA) and the Chief Financial Officers (CFOs) Act of 1990.

Circular A-130, *Management of Federal Information Resources* - This Circular establishes policy for the management of Federal information resources in accordance with the Computer Security Act of 1987.

Circular A-130, Appendix III, *Security of Federal Automated Information Resources* - This Appendix establishes a minimum set of controls to be included in Federal automated information security programs. It also assigns Federal agency responsibilities for the security of automated information and incorporates requirements of the Computer Security Act of 1987 and responsibilities assigned in applicable national security directives.

OMB Memoranda pertaining to IT security and management:

M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 30, 2003)

M-06-14, OMB Guidance Planning for the President's Fiscal Year 2008 Budget Request

M-06-15, OMB Guidance Safeguarding Personally Identifiable Information

M-06-16, OMB Guidance Protection of Sensitive Agency Information

M-06-19, OMB Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

Department of Energy Orders, Manuals, Notices, and Guidelines
DOE CIO – C-38 Protection of Personally Identifiable Information

NIST Federal Information Processing Standards (FIPS) & Special Publications 800 Series (SP) including:
NIST FIPS-199, Standards for Security Categorization of Federal Information and Information Systems

NIST FIPS-200, Minimum Security Requirements for Federal Information and Information Systems

NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems

NIST SP 800-30, Risk Management Guide for Information Technology Systems

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems

NIST SP 800-53, Recommended Security Controls for Federal Information Systems

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories