September 19, 2006

MEMORANDUM TO: Those on the Enclosed List

FROM: Luis A. Reyes ***/RA Martin J. Virgilio Acting For/***
Executive Director for Operations

SUBJECT: PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

In a June 23, 2006, memorandum (—06-16), "Protection of Sensitive Agency Information," the Office of Management and Budget (OMB) recommended that the heads of all departments and agencies encrypt all data on mobile computers and devices that carry agency data unless their Deputy Secretary or designate determines, in writing, that the data is non-sensitive. OMB further recommended that agencies allow remote access only with two-factor authentication when a device separate from the computer gaining access provides one of the factors and that agencies use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity. Additionally, OMB recommended that agencies log all computer-readable data extracts holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. OMB later clarified that the intent of the memorandum was to focus on personally identifiable information (PII).[1]

In response to the OMB recommendations, effective with the date of this memorandum, I am issuing the following direction that will also be issued to the NRC staff via a Yellow Announcement:

1. Because we do not currently have the mechanisms to encrypt data on mobile computers or devices, the Nuclear Regulatory Commission (NRC) is prohibiting the removal of electronic PII from NRC-controlled space until all PII on mobile computers or devices is encrypted. Additionally, the staff is prohibited from placing PII pertaining to NRC official business on personally-owned hard drives, removable media, and other stand-alone storage devices and must delete any existing PII from such equipment within the next 30 days. The staff is also

CONTACT: Russell A. Nichols, IRSD/OIS
301-415-6874

[1] For the purposes of the protections and prohibitions described in this memorandum, personally identifiable information is information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual (i.e., a person's name, in combination with any of the following information: relatives names, postal address, home email address, home or cellular telephone number, personal characteristics, Social Security number, date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or other information that would make the individual's identity easily traceable.)

prohibited from using personally-owned computers for processing or storing PII of individuals pertaining to NRC official business other than themselves. The staff is prohibited from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted. In cases in which it is necessary to take unredacted documents outside NRC-controlled space, office directors or regional administrators or their designees may issue exceptions. However, the exceptions must be in writing, describe why unredacted documents are necessary, and describe how the documents will be protected while outside NRC-controlled space. These exceptions should be granted infrequently and a copy of the written exception must be provided to the Director, Office of Information Services (OIS). This direction does not prohibit the removal or use of emergency contact information outside NRC-controlled space; an exception is not required.

2. NRC remote broadband access through Citrix implements two-factor authentication by requiring two separate object authentications to obtain access to the NRC remote access services: (1) a digital certificate and (2) a user name and password. The user name and password are not stored on the workstation and are independent of the digital certificate authentication. However, it does not meet the criterion for "a device separate from the computer gaining access." Because the risk associated with the lack of a separate device is low, I endorse access to PII through Citrix broadband at this time. The staff will be further evaluating the use of a separate device as part of our long-term actions.

   In the interim, the staff is prohibited from accessing systems containing PII through a dial-up modem unless they use an NRC laptop that is configured in accordance with security requirements approved by OIS. This prohibition does not apply to employees remotely accessing the Human Resources Management System or Employee Express to update their own personal information.

3. NRC's Remote Access System invokes a forced logout after 30 minutes of user inactivity. BlackBerry handheld devices have a system-enforced logout after 15 minutes of inactivity. Other mobile remote access devices, such as Palm Pilots, currently do not employ consistent timeout functions.

   All mobile devices on which PII is stored must be password-protected within 30 days of issuance of this guidance and, where possible, lockout after 30 minutes (or less) of user inactivity. Furthermore, the staff is prohibited from downloading PII pertaining to NRC official business to these mobile remote access devices unless these measures are in place or authorization to do so has been given. If there is existing PII on mobile remote access devices where password protection is not in place, the staff must remove PII from such devices within 30 days.

   Email that is transmitted outside of NRC's Local Area Network/Wide Area Network (LAN/WAN) via the Internet can be read in transit. I recognize that the

staff cannot be held accountable for email received that might contain PII; however, except where necessary to conduct agency business, the staff is prohibited from sending email containing PII outside the agency. Emailing PII within the NRC LAN/WAN is acceptable, including to and from BlackBerry handheld devices interacting within NRC's email system.

4. NRC has many Privacy Act Systems of Records from which Federally-owned information is retrieved by name or unique identifier and for which Systems of Records Notices have been published in the *Federal Register*. Managers of these Systems of Records will be instructed that within 30 days of issuance of my guidance, access to systems containing PII must be reviewed and limited to staff with a need to know. In addition, within 60 days, the managers must identify existing extracts or outputs that contain PII and determine whether the extracts are still necessary. System owners are required to log all computer-readable data extracts from these systems holding PII and verify that each extract, including PII, has been erased within 90 days or that its use is still required. For systems that cannot automatically generate logs of data extracts, manual logs must be maintained. OIS will develop a plan to identify any other systems that store PII, specifically extractable PII. The control of downloading PII will be included in the staff training mentioned later in this document.

The NRC has initiated improvements related to the protection of PII, as well as information security as a whole. The Chief Information Officer directed offices in a June 21, 2006, memorandum to identify PII contained in personal files and productivity tools such as spreadsheets or databases (ADAMS Accession No. ML061580636). OIS provided the offices with an automated tool to assist the staff in searching and identifying documents with PII. The work required to search all of the shared drives is much more labor-intensive and of a greater magnitude than originally anticipated, and as a result, the original due date of September 15, 2006 has been generically extended to December 29, 2006. OIS is working to reduce the reporting burden on offices. Although the due date has been extended, I am reiterating the importance of completing this activity.

Documents containing PII of NRC employees and external parties were recently found in the ADAMS Publicly Available Records System (PARS). The documents have been removed, and we are nearing completion of notifying all of the affected parties. To ensure that PII is not made publicly available through the PARS, remind staff of their responsibility to review documents they submit to ADAMS for public release and to redact PII contained in them.

In conjunction with the Office of Administration (ADM), OIS will ask contract project managers (PMs) to have current contractors inventory PII in their possession. PMs then must determine the contractor's need to possess the PII. When a PM cannot establish the necessity to possess PII data, OIS, ADM, and the PM will coordinate with the contractor to ensure the proper collection, handling, and disposal of the PII. Also, OIS will create an interoffice task force to determine the business processes that include PII, including data collection resulting from NRC Information Collections and NRC forms, and to revise agency direction, as appropriate, on the use of PII.

In addition, the Commission recently issued a Staff Requirement Memorandum requesting modification to the agency's Sensitive Unclassified Non-Safeguards Information (SUNSI) policy. Until this is done, the staff should continue to implement the current SUNSI policy, as modified by this memorandum.

cc: Chairman Klein
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons

In addition, the Commission recently issued a Staff Requirement Memorandum requesting modification to the agency's Sensitive Unclassified Non-Safeguards Information (SUNSI) policy. Until this is done, the staff should continue to implement the current SUNSI policy, as modified by this memorandum.

cc: Chairman Klein
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons

DISTRIBUTION:

L. Reyes, EDO	W. Dean, AO	Cyr/Burns	J. Linehan, OIS	T. Rich, OIS	K. Lyons-Burke, OIS
W. Kane, DEDR	K. Olive, OEDO	E. Baker, OIS	J. Golder, OIS	R. Mitchell, OIS	OIS r/f
M. Virgilio, DEDMRS	M. Malloy, OEDO	K. Greene, OIS			
J. Silber, DEDIA	OEDO-2006-0284	06-305 (CIO)			

ADAMS Package No: ML062190452
ADAMS Accession No: ML062010292
ADAMS Document Title: G20060668/OEDO-2006-0284 - Memo to Office Directors and Regional Administrators from L. Reyes, EDO - Protection of Personally Identifiable Information

*see previous concurrence

OFFICE	Tech Editor	OIS/IRSD	OIS/IRSD	OIS/IRSD	DD/OIS	D/OIS	DEDIA	EDO
NAME	HChang: **HC**	**MJanney:JMG for** *	JGolder:**JMG***	JLinehan: **JJL***	KGreene:**KOG**	EBaker:**ETB**	JSilber:TEH	LReyes:MJV
DATE	7/20/06	08/08/06	08/08/06	08/28/06	08/31/06	09/05/06	09/19/06	09/19/06

OFFICIAL RECORD COPY

MEMORANDUM TO THOSE ON THE ENCLOSED LIST DATED:

SUBJECT: PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION IN INFORMATION TECHNOLOGY SYSTEMS

	Mail Stop	
John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste	T-2	E26
E. R. Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel	T-3	F23
Karen D. Cyr, General Counsel	O-15	D21
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication	O-16	C1
Jesse L. Funches, Chief Financial Officer	T-9	F4
Hubert T. Bell, Inspector General	T-5	D28
Janice Dunn Lee, Director, Office of International Programs	O-4	E21
Rebecca L. Schmidt, Director, Office of Congressional Affairs	O-16	C1
Eliot B. Brenner, Director, Office of Public Affairs	O-2	A13
Annette Vietti-Cook, Secretary of the Commission	O-16	C1
Luis A. Reyes, Executive Director for Operations	O-16	E15
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO	O-16	E15
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO	O-16	E15
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO	O-16	E15
Michael R. Johnson, Assistant for Operations, OEDO	O-16	E15
Timothy F. Hagan, Director, Office of Administration	T-7	D26
Cynthia A. Carpenter, Director, Office of Enforcement	O-14	E1
Guy P. Caputo, Director, Office of Investigations	O-3	F1
Edward T. Baker, Director, Office of Information Services	T-6	F15
James F. McDermott, Director, Office of Human Resources	T-3	A2
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards	T-8	A23
James E. Dyer, Director, Office of Nuclear Reactor Regulation	O-5	E7
Brian W. Sheron, Director, Office of Nuclear Regulatory Research	T-10	F12
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights	T-2	C2
Janet R. Schlueter, Director, Office of State and Tribal Programs	O-3	C10
Roy P. Zimmerman, Director, Office of Nuclear Security & Incident Response	T-4	D22a
Samuel J. Collins, Regional Administrator, Region I	RGN-I	
William D. Travers, Regional Administrator, Region II	RGN-II	
James L. Caldwell, Regional Administrator, Region III	RGN-III	
Bruce S. Mallett, Regional Administrator, Region IV	RGN-IV	