August 22, 2006

MEMORANDUM TO: Chairman Klein

FROM: Luis A. Reyes **/RA/**
Executive Director for Operations

SUBJECT: PROTECTION OF PERSONAL PRIVACY INFORMATION

Your memo dated July 26, 2006, asked the staff to take several actions regarding the protection of personally identifiable information (PII).[1]

The U.S. Nuclear Regulatory Commission (NRC) has initiated improvements related to the protection of PII, as well as information security as a whole. These improvements address short-term, mid-term, and long-term goals for NRC's management of PII and overall information security posture. In the short-term, we plan to focus on improving NRC staff awareness, reviewing and updating current NRC direction to reflect the new Office of Management and Budget (OMB) recommendations related to PII, and assisting offices in identifying current data sources with PII information. The mid-term activities focus on implementing mitigation strategies to protect such information from unauthorized use. The long-term goals are updating Management Directive (MD) 12.5, "NRC Automated Information Security Program," to reflect PII direction; identifying, protecting, and monitoring access to PII through completion of Certification and Accreditation (C&A) of NRC's major systems; and designing, developing, and implementing a uniform Enterprise Security Architecture (ESA) based upon Federal and commercial "best practices." The ESA will address all known security requirements (e.g., Homeland Security Presidential Directive 12 (HSPD-12), E-authentication, two-factor authentication, encryption, PII, and mobile computing including BlackBerry handheld devices and telecommuting) and will ensure all systems and applications implement security in a consistent and uniform manner.

CONTACT: Margie Janney, OIS/IRSD
301-415-7245

[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.)

The staff has conducted a thorough review of documents in the Agencywide Documents Access and Management System (ADAMS) to identify and secure individuals' social security numbers (SSNs). All current and former NRC employees whose SSNs were available in the Publicly Available Records System (PARS) library have been notified. The staff is in the process of finalizing notification letters to the entities who submitted the documents with SSNs to PARS. The staff is also working on identifying and notifying the non-NRC staff whose SSNs were made available in NRC correspondence. The documents containing PII were removed from PARS immediately. In addition, the microfiche containing the documents were removed from the Headquarters and Regional Nuclear Document System (NUDOCS) collections. The staff is in the process of ensuring that the microfiche is removed from the Local Public Document Rooms. The staff also notified OMB and the Department of Homeland Security (DHS) about the PII contained in documents placed on PARS.

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). The Office of Information Services (OIS) has provided the offices with an automated tool to assist the staff in searching and identifying documents with PII.

On June 22, 2006, the Director of OIS issued an announcement to all NRC employees and onsite contractors reminding them of their responsibilities to safeguard personal privacy information from unauthorized access (ADAMS Accession Number ML061660137).

OIS' Chief Enterprise Architect is researching the efforts other Federal agencies are taking to protect privacy information. In particular, the staff is obtaining information from the National Institutes of Health (NIH) and the Department of Defense (DoD), and also is looking at non-public entities.

OMB's June 23, 2006, memorandum (M 06-16), "Protection of Sensitive Agency Information," recommends that all agencies take four actions focused on PII:

1. Encrypt all data on mobile computers or devices that carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he or she may designate in writing.

2. Allow remote access only with two-factor authentication when one of the factors is provided by a device separate from the computer gaining access.

3. Use a "timeout" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity.

4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

I will issue the following direction to the staff in response to OMB's memorandum:

1. Because we do not currently have the mechanisms to encrypt data on mobile computers or devices, 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 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, 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." I endorse the staff's view that the risk associated with the lack of a separate device is low, and 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 my guidance and, where possible, lockout after 15 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.

Short-term Planning

As stated previously, our short-term efforts are focused on improving NRC staff awareness of PII, as well as updating direction to incorporate the OMB-recommended guidance related to PII. We are currently updating computer security training to reflect PII data requirements. OIS recently awarded a contract for mandatory instructor-led training of all NRC staff on the topic of information systems security, and PII is extensively addressed. This mandatory training will be conducted between October 2006 and January 2007.

OIS will develop a detailed plan and schedule to complete a comprehensive review of the ADAMS Main and Public Libraries to identify and secure documents containing PII other than SSNs.

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.

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. The task force will identify the

security vulnerabilities of using PII, both for the NRC and our licensees. The task force also will identify actions to mitigate these vulnerabilities, minimize the use of this information, and eliminate its unnecessary use. It needs to be recognized that identification of some vulnerabilities may not be revealed until the C&A process is complete in 2009, as discussed further in this document. NRC's PII direction will recognize that exceptions with minimal risk will be necessary and will include the controls required to allow such exceptions. While the task force will be created in the short term, its efforts will extend into the long term. Contractor assistance may be necessary to minimize the impact on staff.

Mid-term Planning

With regard to mid-term objectives, OIS is evaluating major systems that use PII. OIS is consolidating its Automated Inventory System (AIS) in order to further ensure all systems that utilize PII have been identified and are appropriately managed. As part of its C&A efforts, OIS will assess all identified systems upon their stated need and the vulnerabilities that the use of PII introduces. OIS will also develop mitigation techniques to eliminate PII where possible on agency systems identified or to ensure that PII is managed in a safe and secure manner.

Long-term Planning

For the long-term, OIS is in the process of updating MD 12.5 to reflect the latest PII guidance as recommended in OMB M 06-16. All information technology (IT) security policy will reside in MD 12.5.

OIS is re-engineering NRC's current Security Architecture to improve its ability to identify, protect, and monitor access to sensitive information, including PII. This approach is consistent with the recently published Federal Enterprise Architecture Security and Privacy Profile (FEA SPP) methodology. Additionally, OIS is evaluating industry and Federal "best practices" to assist in the development of an ESA that is "roles-based" and "policy driven."

The agency's recently implemented C&A process will eventually resolve PII issues within existing systems and systems under development, through its Privacy Impact Assessment, Security Characterization, Risk Assessment, Systems Test and Evaluation, Contingency Planning, and Annual Self Assessment processes. These processes have been closely aligned with Federal Information Processing Standards (FIPS) Publication (PUB) 200, "Minimum Security Requirements for Federal Information and Information Systems," and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems." Because this effort will not be completed until 2009, the agency should consider allocating additional resources to analyze the options available and to accelerate the identification of PII data, vulnerabilities, and potential solutions.

NRC does not centrally purchase or control laptops. Currently, offices are allowed to acquire laptops through a purchase card. Operating systems, software, firewalls, and encryption on office laptops are not controlled. To address OMB's recommendation for encryption, one solution would be to replace desktops with dockable laptops in a phased plan; those staff who work most frequently with PII would be the first supplied with dockable laptops. OIS is expecting to begin the development of a laptop-based architecture within the next year. However, the implementation of this effort will occur over the long term.

Resource Estimates

All of the following resource estimates are preliminary and beyond those requested in the fiscal year (FY) 2007 and FY 2008 budgets. As we carry out the activities described above, the staff will work with the Chief Financial Officer to refine these resource estimates.

Short-term Resource Estimates

All efforts in the short-term will use current funding and will be performed by current staff.

Mid-term Resource Estimates

It is anticipated that $250,000 and 3 FTEs will be required in FY 2007 and FY 2008 to design and develop an ESA implementation plan, which also will address PII and OMB-recommended guidance.

In FY 2007 and FY 2008, 2 FTEs will be required to implement the enhanced Privacy Program to support the activities described above and to search and monitor ADAMS for various types of PII.

One FTE is required to address issues related to digital certificate issuance and maintenance in FY 2007 and FY 2008.

Based on the staff's preliminary analysis, we expect there will be a need for additional resources due to the PII that has been extracted from agency systems and the extent to which agency business processes need to be re-engineered. Once the task force has the opportunity to evaluate the magnitude of the issues involved, we will provide you this information.

Long-term Resource Estimates

Specific costs associated with ESA implementation are unknown. However, based upon knowledge and experience from previous agency implementation efforts, OIS anticipates that an additional $1.5 million for ESA implementation will be required in FY 2008.

The cost to integrate existing legacy systems into the ESA will need to be addressed on a case-by-case basis. Additionally, the cost of integrating legacy systems will be funded as a part of system modernization or upgrade efforts.

The following table summarizes our known projected additional resource requirements.

	FY 2007 ($K)			FY 2008 ($K)		
	FTE	**Salary and Benefits Conversion ($)**	**Contract $**	**FTE**	**Salary and Benefits Conversion ($)**	**Contract $**
Mid-Term	6	828	250	6	848	250
Long-Term	-	-	-	-	-	1500
Total	6	828	250	6	848	1750

As requested in your July 26, 2006, memorandum, the Commission will be kept advised of the progress in achieving these goals.

cc: Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons
SECY
OGC
CFO
OIG

The following table summarizes our known projected additional resource requirements.

	FY 2007 ($K)			FY 2008 ($K)		
	FTE	Salary and Benefits Conversion ($)	Contract $	FTE	Salary and Benefits Conversion ($)	Contract $
Mid-Term	6	828	250	6	848	250
Long-Term	-	-	-	-	-	1500
Total	6	828	250	6	848	1750

As requested in your July 26, 2006, memorandum, the Commission will be kept advised of the progress in achieving these goals.

cc: Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons
SECY
OGC
CFO
OIG

DISTRIBUTION:

L. Reyes, EDO	M. Johnson, AO	E. Baker, OIS	R. Mitchell, OIS	OIS r/f	06-338 (CIO)
W. Kane, DEDR	Cyr/Burns, OGC	K. Greene, OIS	T. Rich, OIS	G20060668	
M. Virgilio, DEDMRS	H. Bell, IG	J. Linehan, OIS	EDO r/f	OEDO-2006-0284	
J. Silber, DEDIA	J. McDermott, HR	J. Golder, OIS			
J. Funches, CFO	T. Hagan, ADM	J. Gray, OGC			

ADAMS Package No.: ML062190452
ADAMS Accession No: ML062150504
ADAMS Document Title: G20060668/ OEDO-2006-0284 - Memo to Chairman Klein from L. Reyes, EDO - Protection of Personal Privacy Information

*see previous concurrence

OFFICE	Tech Editor	OIS/IRSD	OIS/IRSD	OIS/IRSD	DD/OIS
NAME	HChang: *HC	MJanney:	JGolder: **JMG**	JLinehan: **JMG for**	KGreene: **KOG**
DATE	08/ 07 /06	08/ /06	08/ 08 /06	08/ 08 /06	08/ 08 /06
OFFICE	D/OIS	DEDIA	EDO	OGC	
NAME	EBaker: **KOG for**	JSilber: THagan Acting for	LReyes:	J. Gray (NLO w/changes)	
DATE	08/ 08 /06	08/22/06	08/22/06	08/18/06	

OFFICIAL RECORD COPY