July 21, 2006

MEMORANDUM TO: Chairman Klein
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons

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

SUBJECT: STAFF REQUIREMENTS MEMORANDUM COMSECY-05-0054 - POLICY REVISION: HANDLING, MARKING, AND PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION

In the subject staff requirements memorandum (SRM), the Commission directed the staff to recommend any necessary revisions to the Sensitive Unclassified Non-Safeguards Information (SUNSI) policy in view of the agency's receipt of the Office of Management and Budget's (OMB's) June 23, 2006, "Memorandum for the Heads of Departments and Agencies," concerning safeguarding of information while using information technology (IT).

The OMB memorandum advised agencies to properly safeguard Personally Identifiable Information (PII)[1] while using IT when information is removed from or accessed from outside the agency location. The OMB attached a checklist from the National Institute of Standards and Technology (NIST) for the protection of remote information. The NRC staff is addressing all of the NIST checklist items as part of NRC's Certification and Accreditation process for IT systems. OMB also recommended that agencies take the following actions:

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

[1]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 (e.g., name, relatives names, postal address, email address, home or cellular telephone number, personal characteristics, Social Security number, place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or information that would make the individuals' identity easily traceable).

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

2. Only allow remote access with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

3. Use a "time-out" 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 confirm that the staff still requires the use of the data or verify that each extract, including sensitive data, is erased within 90 days.

OMB intends to work with the Inspectors General community to review these items as well as the checklist to ensure agencies are properly safeguarding PII.

In an e-mail from Glenn R. Schlarman, OMB, to Edward Baker, Office of Information Services (OIS), on June 28, 2006, Mr. Schlarman clarified that the intent of the OMB memorandum is to "focus on personally identifiable" information, versus the broader category of sensitive information. A copy of the email is enclosed.

With respect to the actual effects on SUNSI policy proposed in the SRM, it is our understanding that NRC will have to add a third tier to the SUNSI Policy in order to respond to the OMB implementation requirement of unique handling for PII. The current SUNSI policy does not require encryption of SUNSI information on mobile computers/devices nor does it require two-factor authentication for remote access, where one of the factors is provided by a device separate from the computer gaining access.[2]

With respect to the Commission direction to continue implementation of the existing SUNSI policy until a new policy is in place, the staff recommends policy to prohibit the removal of PII from NRC-controlled space and will prohibit remote access to PII from home or by mobile computers/devices until such time the agency can implement the OMB recommendations in full. Specifically, PII should be prohibited from being removed from NRC-controlled space until all sensitive data on mobile computers/devices is encrypted and two-factor authentication is provided for remote access.

Of the four recommendations identified above, NRC partially complies with only the third recommendation. NRC's Remote Access System invokes a forced logout after 30 minutes of user inactivity. Mobile devices currently do not have consistent time-out functions. OIS is currently evaluating the remaining new recommendations and will be developing a plan to address them. A draft of an initial plan is expected to be completed within 45 days from

[2]NRC implements two-factor authentication for remote broadband access. However, the second factor, the digital certificate, resides on the computer gaining access.

June 23, 2006 (date of the OMB memo). Additionally, the effects of the OMB requirements must be incorporated into SUNSI policy.

If you have any questions, please contact Russell A. Nichols at 301-415-6874 or via e-mail at RAN2@nrc.gov.

Enclosure:
As stated

cc: OGC
OCA
OPA
CFO
SECY

June 23, 2006 (date of the OMB memo). Additionally, the effects of the OMB requirements must be incorporated into SUNSI policy.

If you have any questions, please contact Russell A. Nichols at 301-415-6874 or via e-mail at RAN2@nrc.gov.

Enclosure:
As stated

cc: OGC
OCA
OPA
CFO
SECY

Distribution:

L. Reyes, EDO	J. Silber,	EDO r/f	J. Linehan,	R. Mitchell,	06-311 (CIO)
W. Kane,	DEDIA	E. Baker, D/OIS	OIS/IRSD	OIS/BPIAD	06-330 RFPSB
DEDR	W. Dean, AO	K. Greene,	J. Golder,	K. Lyons-Burke,	
M. Virgilio,	K. Olive, OEDO	DD/OIS	OIS/IRSD	OIS	
DEDMRS			T. Rich,	OIS r/f	
			OIS/ICOD		

ADAMS Accession No: ML061930029
ADAMS Document Title: Memo to The Commissioners from L. Reyes, EDO - Staff Requirements Memorandum - COMSECY-05-0054 - Policy Revision: Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information

OFFICE	Tech Editor	OIS/IRSD	OIS/IRSD	OIS/IRSD	OIS/IRSD
NAME	HChang: HC	RNichols: RN	MJanney: MJ	JGolder: JG	JLinehan: JL
DATE	07/12/06	07/14/06	07/14/06	07/14/06	07/14/06

OFFICE	OIS/ICOD	DD/OIS	D/OIS	DEDIA	EDO
NAME	TRich: KP for TR*	KGreene: KG	EBaker: EB	JSilber: JS	LReyes: LR
DATE	07/14/06	07/ 18 /06	07/ 18 /06	07/21/06	07/21/06

OFFICIAL RECORD COPY