

November 27, 2003

Mr. David Lochbaum
Nuclear Safety Engineer
Union of Concerned Scientists
1707 H Street NW, Ste. 600
Washington, DC 20006-3962

Dear Mr. Lochbaum:

This is in response to your letter dated August 14, 2003, in which you raised concerns about controlling access to sensitive but unclassified information relating to the Nation's nuclear power plants.

As we believe you are aware from prior dialogue on security issues, the Nuclear Regulatory Commission (NRC) acknowledges its responsibility associated with the potential disclosure of sensitive information ranging from classified to Official Use Only (OUO) documents and data. To that end, the Offices of the Chief Information Officer, Administration, and Nuclear Security and Incident Response manage programs which are designed to protect certain classes of information from potential compromise.

As an example, following the September 11 terrorist attacks, the NRC redesigned its public Web site to remove potentially sensitive information the agency thought might assist an adversary in an attack against one of the NRC-licensed facilities or activities. NRC employed a systematic process for consideration of materials that should be withdrawn from public access. That process included initial removal of all materials from the Web, consideration of each category of material for re-submittal and finally determining an acceptable threshold for what should remain available on the Web site. Although some of the information removed from the Web site may still be publicly available by other means (i.e., in hard-copy), removal from electronic media such as the Web site was appropriate because it made the information more difficult for an adversary to access.

In a September 30, 2002, response letter to you on this topic, the Office of Nuclear Reactor Regulation, acknowledged the NRC staff and licensees are aware of the need to control information access. However, it must be accomplished in a manner that permits the legitimate, responsible conduct of business. Those goals are not mutually exclusive. Additionally, the Department of Homeland Security is moving forward in establishing a "Sensitive Homeland Security Information" category, designed to protect information below Safeguards Information (SGI), without obstructing legitimate uses.

Regarding the NRC, guidance regarding the control of sensitive information below the SGI threshold is provided in the COMSECY-02-0015 Staff Requirements document, "Withholding Sensitive Homeland Security Information From the Public," which is available on the NRC Web site at the following address:
<http://www.nrc.gov/reading-rm/doc-collections/commission/comm-secy/2002/2002-0015comsrm.html>.

In general, sensitive information is to be controlled by the NRC and licensees in accordance with Section 2.790(d) of Title 10 of the Code of Federal Regulations.

The integrity of personnel with information access, whether they be employees or contractors, is integral to information security. To the extent possible, the NRC has enhanced access control requirements in the implementing procedures for the Order on Access Authorization issued on January 7, 2003, entitled "Issuance of Order for Compensatory Measures related to Access Authorization." In fact industry guidance for implementing the January 7, 2003 Order, NEI 03-01 states that the purpose of the guidance is to maintain industry programs that provide reasonable assurance that only trustworthy and reliable people will be allowed into protected areas of nuclear power plants and, by inference, protect the information provided by those power plants from unauthorized disclosure either within or outside the power complex.

These requirements and associated guidance, coupled with due diligence and post September 11 awareness, are intended to provide an appropriate layer of protection. Legislation being considered by the Congress would further enhance access authorization protocols. That said, there is no absolute assurance that sensitive information, below the threshold of SGI, at least a portion of which is a subjective assessment, can consistently be effectively segregated. Rather, the NRC and its licensees continue to use reasonable programs, procedures, and guidance to ensure that sensitive information is handled in a legitimate and responsible manner.

If you have further questions, please contact me at your convenience.

Sincerely,

/RA/

Roy P. Zimmerman, Director
Office of Nuclear Security
and Incident Response

In general, sensitive information is to be controlled by the NRC and licensees in accordance with Section 2.790(d) of Title 10 of the Code of Federal Regulations.

The integrity of personnel with information access, whether they be employees or contractors, is integral to information security. To the extent possible, the NRC has enhanced access control requirements in the implementing procedures for the Order on Access Authorization issued on January 7, 2003, entitled "Issuance of Order for Compensatory Measures related to Access Authorization." In fact industry guidance for implementing the January 7, 2003 Order, NEI 03-01 states that the purpose of the guidance is to maintain industry programs that provide reasonable assurance that only trustworthy and reliable people will be allowed into protected areas of nuclear power plants and, by inference, protect the information provided by those power plants from unauthorized disclosure either within or outside the power complex.

These requirements and associated guidance, coupled with due diligence and post September 11 awareness, are intended to provide an appropriate layer of protection. Legislation being considered by the Congress would further enhance access authorization protocols. That said, there is no absolute assurance that sensitive information, below the threshold of SGI, at least a portion of which is a subjective assessment, can consistently be effectively segregated. Rather, the NRC and its licensees continue to use reasonable programs, procedures, and guidance to ensure that sensitive information is handled in a legitimate and responsible manner.

If you have further questions, please contact me at your convenience.

Sincerely,

/RA/

Roy P. Zimmerman, Director
Office of Nuclear Security
and Incident Response

DISTRIBUTION: (NSIR-03-0382)

PMDA R/F DNS R/F J. Crutchley (NSIR-03-0382) R.Rosano0M.Landau
Package: **ML032660877**; Incoming: **ML030370116**; Letter: **ML032660898**

*See previous concurrence

OFC:	NSIR:PMDA	NSIR:DNS	NSIR:DNS	NSIR:PMDA:C	OGC	D:NSIR
NAME:	YChen*	ASilvious*	CNolan/ MB/f *	JDavis*	JGoldberg - NLO	RZimmerman
DATE:	9/24/03	9/30/03	10/9/03	9/24/03	9/29/03 by e-mail	11/27/2003

C = COVER

E = COVER & ENCLOSURE

N = NO COPY

OFFICIAL RECORD COPY