

March 16, 2011

Mr. Charles H. Rose
Nuclear Cardiology Systems, Inc.
5660 Airport Boulevard, Suite 101
Boulder, CO 80301

Dear Mr. Rose:

This letter is in reference to your letter to the U.S. Nuclear Regulatory Commission (NRC) dated January 12, 2011, in which you indicated that your computer system had been compromised by an external, unauthorized source.

We appreciate you bringing this to our attention. While the NRC is concerned about possible cyber attacks on any NRC or Agreement State licensee computer system, our regulatory concern is focused on those systems that either contain sensitive information related to our mission (i.e., classified, safeguards, or sensitive unclassified information), or control critical safety systems. Because of that concern, NRC issued Information Notice 2009-24, "Sources of Information Related to Potential Cyber Security Vulnerabilities," dated October 13, 2009, to a select group of NRC licensees.

Computer systems of organizations with certain words, including "nuclear" in their title appear to be routine targets of unauthorized entry attempts; thus, we are providing you with a link to the Department of Homeland Security United States Computer Emergency Readiness Team's (US-CERT) website <http://www.us-cert.gov>. The site offers an abundance of information, technical and non-technical, about potential threats and vulnerabilities.

Thank you for bringing this information to our attention.

Sincerely,

/RA/

James G. Luehman, Deputy Director
Division of Materials Safety
and State Agreements
Office of Federal and State Materials
and Environmental Management Programs

CERTIFIED MAIL 7006 0810 0005 9659 6378
RETURN RECEIPT REQUESTED

Mr. Charles H. Rose
Nuclear Cardiology Systems, Inc.
5660 Airport Boulevard, Suite 101
Boulder, CO 80301

Dear Mr. Rose:

This letter is in reference to your letter to the U. S. Nuclear Regulatory Commission (NRC) dated January 12, 2011, in which you indicated that your computer system had been compromised by an external, unauthorized source.

We appreciate you bringing this to our attention. While the NRC is concerned about possible cyber attacks on any NRC or Agreement State licensee computer system, our regulatory concern is focused on those systems that either contain sensitive information related to our mission (i.e., classified, safeguards, or sensitive unclassified information), or control critical safety systems. Because of that concern, NRC issued Information Notice 2009-24, "Sources of Information Related to Potential Cyber Security Vulnerabilities," dated October 13, 2009, to a select group of NRC licensees.

Computer systems of organizations with certain words, including "nuclear" in their title appear to be routine targets of unauthorized entry attempts; thus, we are providing you with a link to the Department of Homeland Security United States Computer Emergency Readiness Team's (US-CERT) website <http://www.us-cert.gov>. The site offers an abundance of information, technical and non-technical, about potential threats and vulnerabilities.

Thank you for bringing this information to our attention.

Sincerely,

/RA/

James G. Luehman, Deputy Director
Division of Materials Safety
and State Agreements
Office of Federal and State Materials
and Environmental Management Programs

DISTRIBUTION:
MSSA R/F

ML110750099

| | | |
|------|------------|----------|
| OFF | DILR | DMSSA |
| NAME | CBrown | JLuehman |
| DATE | 3 / 15 /11 | 3 /16/11 |

OFFICIAL RECORD COPY