January 15, 2010

MEMORANDUM TO: Melvin M. Leach, Director
Division of Preparedness and Response
Office of Nuclear Security and Incident Response

FROM: Richard P. Correia, Director */RA/*
Division of Security Policy
Office of Nuclear Security and Incident Response

SUBJECT: EMERGENCY RESPONSE DATA SYSTEM AND CYBER SECURITY

Recently your staff inquired as to whether Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communication Systems and Networks," applies to Emergency Response Data System (ERDS) equipment that is physically located at licensed nuclear facilities or at aggregation sites designated and controlled by licensees. 10 CFR 73.54 requires, in part, that licensees provide high assurance that their systems, networks, or equipment associated with emergency preparedness (EP) functions of a nuclear facility are adequately protected from cyber attacks. Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," (January 2010) provides clarifying guidance regarding the scope of digital assets that are within the scope of 10 CFR 73.54.

The Division of Security Policy (DSP) staff understands that ERDS is a direct, near real-time electronic data link between a licensee's onsite computer system and the NRC Operations Center that supplements the existing voice transmission capability via the Emergency Notification System. The DSP staff also recognizes that ERDS is undergoing a transition from the use of "dial up" modems to internet-based Virtual Private Network Technology (VPN). The DSP staff further understands that the NRC provides ERDS equipment (e.g., such as modems or electronic data transmitting devices) to power plant licensees for transmitting a limited data set of selected plant parameters listed in 10 CFR 50 Appendix E (VI) "Emergency Response Data Systems," to the NRC Operations Center during certain emergency events, and that these modems or electronic devices are part of Federal systems.

Because ERDS is a Federal information system, its components are considered "government furnished equipment." As a result, NRC-provided ERDS equipment and components are excluded from the scope of "digital computer and communications systems and networks" defined within 10 CFR 73.54(a)(1). NRC-provided ERDS equipment is, however, subject to the security requirements set forth under the Federal Information Security Management Act of 2002 (FISMA), consistent with other Federal computer and communication systems. The NRC is responsible for demonstrating that its computer systems are compliant with FISMA.

CONTACT: Lee Eric, DSP/ISCPB
(301) 415-8099

In addition, the DSP staff notes that the primary intent of the 10 CFR 73.54 regulations is to ensure that licensees provide adequate protection for digital computer and communication systems and networks whose failure or compromise from cyber attack could lead to radiological sabotage event. The secondary intent, in part, is a defense-in-depth measure; that is, to ensure that systems associated with EP-related functions are similarly protected. Consistent with RG 5.71, the scope of systems associated with EP functions that should be considered as being within the scope of 10 CFR 73.54 are those whose failure or compromise would result in a "reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency." Because ERDS is a system designed only to provide nuclear facility data to the NRC in the event of a declared emergency at a licensee site, the DSP staff has determined that its failure or compromise due to a cyber attack would not reduce a licensee's capability to implement appropriate protective measures in the event of an emergency. As such, ERDS would not be considered to be within the scope of 10 CFR 73.54.

Notwithstanding the above, the DSP staff expects that a licensee's cyber security assessment of the computer system from which ERDS receives data (e.g., plant computer, corporate data network) would include an examination of the interface between that system and ERDS, and the potential vulnerabilities presented by a failure or compromise of that interface due to a cyber attack. When conducting this assessment, licensee's can be assured that, consistent with FISMA requirements, the NRC has established multiple levels of protection on the ERDS system. Specifically, in order for an external cyber attack on ERDS to reach the licensee's ERDS interface, all of the following would have to occur:

-compromise the strong encryption of the communication stream within the VPN
-bypass the required IT certificate for connection to the ERDS equipment
-answer two levels of complex password challenges on the ERDS equipment
-reprogram the ERDS equipment to allow bi-directional communication on that interface

If you have any questions about the content of this memorandum, please contact me or my appropriate technical staff.

In addition, the DSP staff notes that the primary intent of the 10 CFR 73.54 regulations is to ensure that licensees provide adequate protection for digital computer and communication systems and networks whose failure or compromise from cyber attack could lead to radiological sabotage event. The secondary intent, in part, is a defense-in-depth measure; that is, to ensure that systems associated with EP-related functions are similarly protected. Consistent with RG 5.71, the scope of systems associated with EP functions that should be considered as being within the scope of 10 CFR 73.54 are those whose failure or compromise would result in a "reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency." Because ERDS is a system designed only to provide nuclear facility data to the NRC in the event of a declared emergency at a licensee site, the DSP staff has determined that its failure or compromise due to a cyber attack would not reduce a licensee's capability to implement appropriate protective measures in the event of an emergency. As such, ERDS would not be considered to be within the scope of 10 CFR 73.54.

Notwithstanding the above, the DSP staff expects that a licensee's cyber security assessment of the computer system from which ERDS receives data (e.g., plant computer, corporate data network) would include an examination of the interface between that system and ERDS, and the potential vulnerabilities presented by a failure or compromise of that interface due to a cyber attack. When conducting this assessment, licensee's can be assured that, consistent with FISMA requirements, the NRC has established multiple levels of protection on the ERDS system. Specifically, in order for an external cyber attack on ERDS to reach the licensee's ERDS interface, all of the following would have to occur:

-compromise the strong encryption of the communication stream within the VPN
-bypass the required IT certificate for connection to the ERDS equipment
-answer two levels of complex password challenges on the ERDS equipment
-reprogram the ERDS equipment to allow bi-directional communication on that interface

If you have any questions about the content of this memorandum, please contact me or my appropriate technical staff.

ADAMS ACCESSION NO.: ML100130359

OFFICE	NSIR/DSP/ISCPB	NSIR/DSP/ISCPB	NSIR/DSP/DDRS
NAME	E.Lee	C.Erlanger	S.Morris for R.Correia
DATE	1/13/2010	1/ /2010	1/15/2010