January 3, 2007

SECURITY ADVISORY FOR POWER REACTORS

SA-07-01

SUBJECT: USE OF AUTHENTICATION CODES TO VALIDATE CALLER IDENTIFICATION DURING IMMINENT THREATS AND PHYSICAL ATTACKS

The U.S. Nuclear Regulatory Commission (NRC) has identified the need to expedite the verification of caller identity in the case of an imminent threat to a nuclear power plant. This is especially important in the case of an imminent airborne threat.

Background

The current reporting requirements for security-related events are found in 10 CFR 73.71, Appendix G, "Reportable Safeguard Events." Additionally, the Commission has previously advised licensees of the need to expedite their initial notifications to the NRC in NRC Bulletin 2005-02 "Emergency Preparedness and Response Actions for Security-Based Events," dated July 18, 2005.

The current verification protocol is as follows: NRC receives threat information from an external source (e.g., the North American Aerospace Defense Command and the U.S. Northern Command) and telephones the licensee. In order to verify that the caller is actually the NRC, the licensee has two options: (1) While the licensee stays on the line, another member of the licensee's staff can call the NRC Operations Center to verify the authenticity of the call; or (2) The licensee can hang up the phone and call the NRC Operations Center to perform the verification. This process is performed similarly if the licensee calls the NRC Operations Center to make a notification of an imminent or actual security threat.

The current verification protocol requires the use of resources that are better suited to other tasks, such as notifying additional State and local first responders. Additionally, this protocol could delay licensees' actions in an imminent threat response environment. Therefore, NRC will use an authentication code with its licensees to verify a caller's identity whenever a caller makes an imminent threat notification. The proper use of the code will provide a short, simple means of call authentication that will eliminate the need to perform a call back and will still maintain reasonable assurance of the caller's identity.

Discussion

Proposed Authentication Code Process

NRC will generate and provide a single, four-digit alphanumeric sequence to each main control room during the daily plant status communications check at 4:00 AM Eastern Time (ET). The NRC will state the current authentication code and then give the new authentication code. The codes will go into effect each day at 8:00 AM. In the event of an imminent threat notification prior to 8:00 AM ET, NRC and the licensee will authenticate the caller using the code that NRC provided the previous day.

NRC has not classified the authentication code as safeguards information. NRC has deemed not classifying the code to be an acceptable risk because of the short life span and limited distribution of each daily code. Although NRC issues only one code at a time, NRC will distribute the authentication code to licensee staff on a “need-to-know” basis to minimize the possibility of caller deception. Generally, distribution will be limited to the control room staff and emergency plan communicators.

Each licensee should develop a process for maintaining the authentication code in a convenient, accessible location to prevent delaying the transfer of information during imminent threat report communications.

Call Process

The call process of reporting an imminent threat from the NRC Operations Center to an affected licensee is described below:

1. NRC Headquarters Operations Officer (HOO) calls the affected licensee.

2. When the licensee answers the phone, the HOO will state it has an Emergency Aircraft Imminent Threat Warning Message or a Nuclear Power Plant Attack Threat Message and give the authentication code.

3. The licensee will verify the code and reply that the licensee is ready to copy the emergency message.

4. If an incorrect code is given, the licensee will hang up, then immediately call back the NRC HOO. No code word will be utilized for the call back.

Example Exchange During an Imminent Threat Report

An example of the expected exchange during an imminent threat report is shown below:

NRC HOO: "This is the NRC Operations Officer, I have an Emergency Aircraft Imminent Threat Warning Message; the authentication code is Alpha One Bravo Yankee."

Licensee: Checks current authentication code, and if correct, responds: "Authentication confirmed; standing by for warning message; go ahead NRC."

This process is similar to NRC’s requirements for a prompt notification (within 15 minutes) by the licensee of an onsite security threat. The report is made, and the authentication code is provided to the NRC Operations Center, allowing additional notifications to other Federal organizations (e.g., Department of Homeland Security).

Summary

Implementation of Authentication Code Process

NRC expects to have this process in place by March 1, 2007. Licensees are requested to develop procedures and train applicable personnel in this process. This is not meant to encumber the licensees with additional requirements, and licensees are encouraged to keep the process as simple as possible.

The NRC HOOs will coordinate and perform pilot phone calls with licensees beginning February 12, 2007. These calls will ensure that the process is working efficiently prior to full-scale implementation.

Backfit Analysis Statement: This Security Advisory requires no action or written response and is, therefore, not a backfit under 10 CFR 50.109. Consequently, the staff did not perform a backfit analysis.

Paperwork Reduction Act Statement: This Security Advisory contains information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget, approval number 3150-0011, which expires February 28, 2007.

The burden to the public for these mandatory information collections is estimated to average 20 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of these information collections, including suggestions for reducing the burden, to the Records and FOIA/Privacy Services Branch (T-5 F52), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0011, or by Internet electronic mail to INFOCOLLECTS@NRC.GOV; and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0011), Office of Management and Budget, Washington, DC 20503.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

Approved by **/RA/**
Roy P. Zimmerman, Director
Office of Nuclear Security and Incident Response

Technical Contact: Jason Kozal
(301) 415-0648
Email: jwk@nrc.gov