POLICY ISSUE
NOTATION VOTE

August 2, 2006 SECY-06-0173

FOR: The Commissioners

FROM: Luis A. Reyes
Executive Director for Operations

SUBJECT: HISTORY OF THE EMERGENCY NOTIFICATION SYSTEM AND OPTIONS TO PROVIDE CONFIRMATION OF AUTHORITY/IDENTITY OF A CALLER

PURPOSE:

In response to the Staff Requirements Memoranda (SRM), M060117, dated February 3, 2006, this paper provides the Commission with the history of the Emergency Notification System (ENS) lines and requests Commission approval of a method to quickly confirm the authority or identity of a caller with respect to the imminent threat and physical attack procedures.

SUMMARY:

The Commission has identified the need to establish a method to quickly confirm the authority/ identity of a caller with respect to an imminent threat. The Emergency Notification System (ENS) provides a reliable voice communication system that allows NRC to communicate with power reactor licensees during an emergency, including an imminent threat. However, the current configuration of ENS will not support caller identification (caller ID). The staff evaluated several alternatives including the restoration of dedicated direct lines (ring downs). Additionally, the staff has provided an update of the communications evaluation (study) that is being undertaken to assess the overall status and health of emergency communications. The staff recommends the Commission approve the use of authentication codes as the method to confirm the authority/identity of a caller in an imminent threat situation. This process is described in Enclosure 2.

CONTACT: Jason Kozal, NSIR/DPR
(301) 415-5776

BACKGROUND:

In the aftermath of the Three Mile Island accident, the U.S. Nuclear Regulatory Commission (NRC) established the Emergency Telecommunications System (ETS) to provide reliable communications between NRC and its power reactor licensees. ETS was composed of multiple communications circuits (e.g., ENS, the Health Physics Network) to each power reactor site. ENS was a ring-down phone system (i.e., direct access between the licensee and the NRC Operations Center without dialing) that terminated at multiple locations on the licensee's end and at the NRC Operations Center. In 1991, due to obsolescence of the equipment and high maintenance costs, the Federal Government replaced the ETS circuits with Direct Access Lines (DALs) to the Federal long distance service. This increased the reliability of the ENS by bypassing the publicly switched network, which can become overwhelmed in an emergency and lead to a disruption in communications. DALs operate similar to a commercial phone, in that a specific phone number must be dialed (e.g., licensee control room to NRC Operations Center) to connect the circuit.

The importance of redundancy and diversity of communications was illustrated by the experience at Davis Besse on June 24, 1998. When a tornado destroyed all modes of telecommunication at the site, only the licensee's corporate microwave system was functional. The control room operators had only one circuit available on that network to communicate with NRC, who subsequently notified the State authorities of the onsite conditions. Based on this event, the NRC staff identified an alternate option to allow enhanced reliability of communications at nuclear power plants. The staff published Regulatory Issue Summary (RIS) 2000-11, "NRC Emergency Telecommunications System," to allow licensees the use of their own corporate telecommunication capabilities, to provide reliable access to long-distance access networks, and to avoid the local telephone company's switch. Currently, approximately 30 percent of licensees use their own corporate communication systems while the remainder continue to use DALs.

A detailed discussion on the system background of the ENS is contained in Enclosure 1.

DISCUSSION:

1.0 Evaluation of Caller ID and the Current ETS Configuration

Caller identification (caller ID) technology used in domestic applications requires modems to supply and receive information specific to the call. A modem is located at the service provider's central office and a modem is incorporated into the call recipient's caller ID device. These devices communicate and transmit the information needed to produce the information display. The NRC Operations Center and the licensees' sites must have powered lines to enable caller ID, which is not supported by the current ETS hardware. Automatic Number Identification (ANI) is similar in nature to caller ID. Phone companies developed ANI to provide automatic billing for long distance services. Similar to caller ID, the NRC Operations Center and the licensees' sites must have powered lines to enable ANI. Although ETS is a two-wire telecommunications system similar to a domestic phone system, the ETS requirement to bypass the local exchange company makes ANI impossible in its current configuration.

2.0 Identification of Alternatives Considered

Using current telecommunications technology, the ability to quickly determine the identity of callers in an imminent attack situation could improve response capabilities. Currently, licensees and the NRC Operations Center cannot identify callers. The current protocol has licensees initiating a second phone call to the NRC Operations Center to verify a caller's identity.

Similarly, in the case of a physical attack on a licensee, the Headquarters Operations Officer (HOO) must initiate a second phone call to the licensee to verify a caller's identity. The current protocol uses time and resources that would be better dedicated to other tasks. The licensee could use this time to more promptly notify additional State and local first responders, establish plant conditions, or take appropriate personnel protective measures. The HOO could use this time to more promptly notify other NRC licensed facilities, notify Commissioners, and notify key NRC senior management, or to implement appropriate imminent or physical attack procedures. In either case, earlier notification or implementation of actions would occur.

The Office of Nuclear Security and Incident Response (NSIR) worked closely with the Office of Information Services (OIS) to research and develop various alternatives to resolve the issue of caller verification and identification with respect to imminent threat and physical attack procedures.

2.1 Authentication Codes Alternative (Implementation Within 6 Months)

An alternative to resolve the issue of caller identification and verification is to establish the use of authentication codes to verify a caller's identity. This program is described in a draft security advisory contained in Enclosure 2. The use of codes provides a short, simple means of call authentication that eliminates the need for a second phone call. The HOO will provide the authentication codes, a random 4-digit alphanumeric sequence, on a daily basis to each main control room during the daily plant status check phone call. The code becomes effective at a prescribed time each day, preventing any confusion in the unlikely event that an imminent threat is identified while NRC headquarters is distributing the codes. There will be one alphanumeric code for all licensees to prevent potential error when communicating a threat to a specific plant. The NRC Operations Center would facilitate and manage this program.

Pros:

- This alternative establishes a level of validation of Caller- ID that currently does not exist.
- This process could be easily implemented in short time period.
- The cost of this alternative would be minimal.
- No rulemaking would be required to implement this program.

Cons:

- This program should have additional vetting with industry prior to implementation.

- This program is not a permanent technological solution.

- There is some impact on resources to maintain the program.

As indicated in the recommendation section, the staff support this alternative for immediate implementation to verify a caller's identity.

The staff has initiated an initial dialogue with the Nuclear Energy Institute (NEI) concerning the development and implementation of this program. The initial outreach included discussion of the periodicity of the code change and implementation strategy, which was received well. The staff will continue this dialogue during the implementation phase if the Commission selects this option.

2.2 Technological Alternatives (Implementation Within 2–3 Years)

The staff evaluated various technological alternatives to resolve the issue of caller verification and identification with respect to imminent threat and physical attack procedures. These alternatives are as follows:

2.2.a Installation of Dedicated Switched Voice Services

Installation of dedicated switched voice services to each of the operating nuclear power plants where an Emergency Notification System (ENS) line is required.

These services would be digital in nature using the Integrated Switched Digital Network (ISDN) Primary Rate Interface (PRI) technology and, like the current direct access lines (DALs), would bypass the local telephone company's switching systems.

Pros

- This system provides for 2-way caller identification (caller ID) technology which allows for instantaneous identification of call origination.

- This technology maintains the diversity of communication routes that exist in the current communication configurations.

- This technology provides a common framework to assure authentication capabilities that can be required of all licensees.

- This technology uses the existing 700 numbers to allow transition without any change in contact information.

- This service is a mature, proven technology that has been used in many applications throughout the public and private sectors.

- This system conforms with the current requirements for the continuity of NRC

operations (COOP) by allowing installation at the NRC's alternate incident response location without any outlay of resources.

- This system has no impact on the NRC Operations Center's current Private Branch Exchange (PBX) initiative.

Cons

- This system is not a secure communications system; therefore, this technology is vulnerable to caller ID "spoofing." Spoofing is the process in which the phone number at the point of call origin is replaced with a number of the caller's choice. Recently, spoofing has been made easier for the general public. Web sites have emerged that allow this spoofing technology to anyone with Internet access. The telephone configuration that currently exists in the NRC Operations Center does make spoofing more difficult, but not impossible; in this case, the caller would have to access the FTS system and be identified as belonging to either the General Services Administration or the NRC billing structure in order to perform a successful "spoof."

- Rulemaking pursuant to 10 CFR 50.72 and 10 CFR 73.71 would be required to provide uninterruptible emergency power to this system at the licensee's locations.

Cost

The initial outlay of resources for equipment and craft is approximately $350,000. Annual recurring costs to NRC would be approximately $200,000.

2.2.b Installation of the Critical Infrastructure Information Warning System (CWIN)

Installation of the CWIN at licensee sites is required.

The Department of Homeland Security (DHS) is responsible for protecting the national infrastructures. DHS is also responsible for ensuring that there is a means to collaborate and coordinate the necessary resources to restore impacted infrastructures in the event information or physical infrastructures are compromised. The CWIN facilitates immediate alert, notification, sharing, and collaboration of critical infrastructure and information within and between the Federal Government and the industry. CWIN provides a technologically advanced, secure network for communication, collaboration, alert, and notification.

Pros

- The DHS CWIN is a survivable, critical communications tool that is dependent neither on the Public Switch Network (PSN) nor the public Internet. CWIN can also communicate both data and voice information in a collaborative environment in support of infrastructure restoration.

- CWIN provides a dependable method of communication and allows NRC to communicate with other Federal agencies, State and local governments, the private

sector, and international organizations in the event that primary methods of communication are unavailable.

- CWIN is already operational in many locations, including all 50 States' Emergency Operations Facilities (EOFs) and the NRC Operations Center.

- CWIN is an independent network that has caller ID and cannot be "spoofed."

- The NRC Incident Response Organization finds CWIN's ability to provide both voice and data transfer capabilities to be highly beneficial to the agency's mission.

Cons

- NRC could be at risk to lose use of this system as DHS is the custodian of CWIN, sets the priorities within CWIN, and controls the allocation of its bandwidth. The staff considers a major risk with this system to be a possible hampering of NRC's communications when a large-scale event (e.g., Hurricane Katrina) is in progress and already using the available bandwidth. This may lead to major delays in communications due to the fact that bandwidth would have to be made available to provide a communication link with a licensee.

- CWIN installation and continuation of operations would involve a significant initial outlay of resources. CWIN installation has the highest front-end cost and the highest recurring cost of any of the options.

- Rulemaking pursuant to 10 CFR 50.72 and 10 CFR 73.71 would be required to provide uninterruptible emergency power to this system.

- The CWIN alternative would require a redesign of the agency COOP plan as current contingencies and processes would not support the CWIN communications path.

Cost

For voice service only, the initial outlay of resources for equipment and craft is approximately $250,000. The annual recurring costs to NRC would be approximately $970,000.

For both voice and data service, the initial outlay of resources for equipment and craft is approximately $530,000. The annual recurring costs to NRC would be approximately $1.35 million. These costs will only support 1 ETS function (i.e., ENS, HPN, or ERDS).

2.2.c Re-establishment of Independent Direct Lines

NRC would require the re-installation of point-to-point, ring-down circuits in the NRC Operations Center, the licensee's site, and the NRC COOP site. The necessary telephone equipment and communications circuits must be installed on the NRC and licensee ends. Two separate circuits must be installed at the licensee's site to allow for communication with both the NRC Operations Center and the COOP sites.

Pros

- This system provides for an instant connection between NRC and its licensees and would solve the issue of caller identification. There would be no confusion as to where the call originated, and this system would eliminate the delay created by the current verification (callback) protocol.

- These lines could be extensions of the NRC Operations Center PBX system and greatly enhance the NRC Operations Center capabilities.

Cons

- This endeavor would be large in scope. This system would require installation of duplicate components in multiple locations to support COOP requirements initiating major changes to all licensees and NRC emergency response plans. Separate circuits would have to be installed at the NRC Operations Center and at the COOP site.

- This system would be difficult to manage during a multiple site, coordinated attack scenario. This system has limited abilities to interface with other NRC Operations Center communications systems.

- This system is not diverse in that a single fault between NRC and the licensee would disable the system for the affected site. Current systems have multiple avenues through which the phone signal can reach the NRC Operations Center. If a natural phenomenon were to affect the circuit path between the licensee and the NRC Operations Center, a reroute of the signal would not be possible causing a loss in communications with the NRC.

- Rulemaking pursuant to 10 CFR 50.72(a) would be required to install these systems in main control rooms.

Cost

The initial outlay of resources for equipment and craft is approximately $560,000. The annual recurring costs to NRC would be approximately $360,000.

2.3 Rulemaking

When evaluating these technological alternatives, the staff determined that rulemaking would be required for alternatives that modified or upgraded the ETS technology. This is due primarily to the requirement to supply an uninterruptible power source to the new telecommunications systems. To institute the new rule, the staff has determined that a timeline of 2–3 years is realistic with an additional 2 years to fully implement the new hardware and services.

3.0 Longer-term Initiatives

3.1 DHS Initiative

Although not an alternative, the staff would like to keep the Commission informed of another DHS initiative. DHS is currently sponsoring a pilot system that is similar in nature to the third technological alternative describing the re-establishment of independent direct lines. This pilot

includes installation of a redundant, diverse phone system for Calvert Cliffs Nuclear Power Plant, Cove Point Liquified Natural Gas Terminal, NRC Operations Center, and the DHS National Infrastructure Coordinating Center (NICC). This system employs technology that allows for authentication of a caller by using caller-ID over an exclusive network. This phone system allows a licensee who is under attack to promptly and simultaneously notify NRC and NICC. This will allow NICC to alert other administrators of critical infrastructure assets in the same area of the attack so they can take actions to protect those assets. The staff will keep the Commission informed of this pilot program.

3.2 Staff Initiative

Currently, the staff has undertaken an initiative designed to develop a telecommunications "roadmap." This product will stimulate a better decision making process to enhance and streamline the budgeting and planning process for the NRC Operations Center. This process would be used to determine the appropriate technology to provide a long term technological solution to the caller authentication issue. The steps of this process is to perform a baseline analysis of existing Operations Center technology, use that data to determine the future needs of the NRC Operations Center and develop a strategic process to implement the necessary changes.

The staff estimates that the current initiative assessment will cost $300,000. This is funded within the FY 2006 budget. The staff will address all enhancements and additional technologies identified in the implementation study in a subsequent paper to the Commission and seek appropriate funding in accordance with the normal budgeting cycle.

COMMITMENT:

None

RECOMMENDATION:

The staff recommends that the Commission approve the staff proposal for the authentication codes alternative discussed in section 2.1 and detailed in the draft security advisory (Enclosure 2).

RESOURCES:

During the development and implementation phase of authentication codes, the NRC staff will use 0.2 FTE. This can be absorbed into the current NSIR budget for reactor event response. After implementation, the maintenance of the program will be part of the HOO daily routine and will have a negligible impact on the required FTE.

COORDINATION:

The Office of the General Counsel reviewed this package and has no legal objection. The Office of the Chief Financial Officer reviewed this package and determined that it has no financial impact.

/RA/

Luis A. Reyes
Executive Director
for Operations

Enclosures:
1. System Background (Detailed) Information on The Emergency Telecommunications System
2. Draft Security Advisory for Affected Operating Power Reactor Licensee and Fuel Cycle Facilities

System Background (Detailed) Information on the Emergency Telecommunications System

In the aftermath of the Three Mile Island (TMI) accident, NRC established two dedicated telephone systems for emergency communications: the Emergency Notification System (ENS) and the Health Physics Network (HPN). The ENS, used by NRC to receive information from licensees on plant safety status, was a ring-down phone system that terminated at four different places on the licensee's end: the Control Room, the Technical Support Center (TSC), the Emergency Operations Facility (EOF), and the NRC Resident Inspector's office. Taking any one of these extensions "off the hook" automatically activated the dedicated circuit to the NRC Operations Center. The HPN, used for conveying radiological and dose projection information, consisted of eight multidrop (similar to a party line) dedicated circuits. Each HPN circuit terminated at a Regional office and at the NRC Operations Center, as well as at all power plants and fuel cycle facilities on each respective loop. In 1987, NRC transferred the unreliable and expensive HPN service from dedicated circuits to the public switched telephone network (PSTN).

ENS initially was designed by AT&T using equipment manufactured by WestCom, Inc. After divestiture, WestCom sold the rights to this equipment and design to Tellabs, Inc. By 1990, Tellabs was no longer manufacturing WestCom equipment, and the existing Tellabs equipment was becoming increasingly unreliable. In addition to these equipment concerns, NRC experienced communication problems during the agency's response to a 1990 event at the Vogtle facility; this raised additional questions as to the operational readiness of ENS.

Consequently by 1990, the cost of maintaining an increasingly obsolete dedicated network exceeded $5 million annually. As a result, the Federal Government included the ENS in the transition to the Federal Telecommunications System (FTS) 2000, Federal long distance service, along with the other emergency communications functions or circuits: HPN, Reactor Safety Counterpart Link (RSCL), Protective Measures Counterpart Link (PMCL), Emergency Response Data System (ERDS) Channel, Management Counterpart Link (MCL), and Local Area Network (LAN) Access. These circuits are known collectively as the Emergency Telecommunications System (ETS). This implementation occurred in 1991–1992 for all nuclear power plant licensees. The direct dedicated line service employed by ENS was discontinued because of the aging and obsolescence of the equipment, and the ENS was replaced by the Direct Access Lines (DALs) to FTS 2000. The move to the FTS for the other communication functions increased the reliability and ensured that each of the emergency communication functions bypassed the local central office of the PSTN, which experience had shown could become overwhelmed in an emergency and disrupt the communication pathway.

In SECY-98-0194, "Upgrading the NRC Operations Center Emergency Telecommunications System," the NRC staff identified options for more efficiently providing ETS services for nuclear power plants. The option supported by the staff and approved by the Commission in Staff Requirement Memorandum (SRM) dated December 9, 1998, involved using preexisting licensee communications networks to provide access to long distance service in a manner that would be independent of the local telephone company's switch. When reviewing the options for a post-FTS 2000 ETS, the staff identified a potential efficiency enhancement. The primary purpose of the DALs is to provide access to long distance networks independent of the local telephone switch. Booz-Allen Hamilton's (BAH's) study and NRC's survey of representative licensee sites indicated that most utilities had established corporate telecommunications

capabilities which already provided independent access to long distance networks (i.e., avoided the local telephone company's switch). Therefore, ETS functionality could be provided over corporate networks at minimal additional cost to licensees; this measure would eliminate the large recurring costs associated with NRC's dedicated circuits. This upgrade was implemented in FY 2001 as part of FTS 2001, a follow-on contract to FTS 2000. The recommendations advanced at that time did not consider a post-9/11 environment; rather, the upgrade focused on maintaining acceptable reliability and minimizing cost. As a result, the current FTS 2001 configurations do not support caller identification due to technical design obstacles, nor is there a requirement for licensee provided back-up power availability.

The staff also met with representatives of the National Communications System (NCS) to solicit recommendations on caller identification and verification capabilities. NCS offered a number of solutions; all of which introduced different communications channels than what the NRC Operations Center was using. At that time, the staff deemed the presented options as too costly.

Further, the staff also evaluated Privatel, a secure telephone device manufactured by L3 communications to assist with caller identification and verification. The device was successfully tested at two licensed facilities (one FTS 2001 and one non-FTS 2001). However, the Privatel device introduced unacceptable time delays in verifying the calls.

In response to an SRM dated August 18, 2004, the staff presented the Commission with several options and an interim solution (valid until the General Services Administration (GSA) Networx acquisitions will be awarded in March and May 2007) in a February 18, 2005, memorandum (see ML050340350). In January 2005, the staff formally requested the GSA include the requirements for caller identification and verification in the GSA-developed request for proposal for the Networx contracts. At the time of the memorandum, the staff believed that Automatic Number Identification (ANI) would function properly in the Networx environment. As an interim measure, the staff has a manual verification protocol between the NRC Operations Center and NRC licensees to provide caller identification and verification. The receiver of the call must initiate a second phone call to verify the caller's identity (i.e., call a different line to verify the origin of the call and to be assured of its authenticity).

Maintaining the current ETS design configuration under Networx will not address the ANI or caller identification issues. If the current configuration is changed, additional costs may be incurred. The staff also recognized that the need to verify callers' identities may extend beyond NRC and its licensees (e.g., when communicating with intelligence, emergency response, or command and control agencies at any level of Government). The configuration of the current phone system is unable to support ANI. Although the ETS system is a two-wire system, similar to a domestic phone system which can support ANI, ETS is configured as a "non-local serving wire center" analog telephone path that makes ANI impossible. For caller ID or ANI to work, modems are used to supply and receive the information. There is a modem at the service provider's central office and a modem incorporated into the call recipient's caller ID device that communicate and transmit the information needed to produce the information display. The NRC Operations Center and the licensees' sites must have powered lines to enable ANI, which is not supported by the current ETS hardware.

DATE

**SECURITY ADVISORY FOR
AFFECTED OPERATING POWER REACTOR LICENSEE
AND FUEL CYCLE FACILITIES**

(SA-0x-xx)

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 (NPP) or fuel cycle facility (FCF). This is specifically important in the case of an imminent airborne threat.

The current process of verification (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 (NORAD/NORTHCOM)) and telephones the licensee. In order to verify that the caller is actually the NRC, the licensee has two options: (1) While the receiver of the call stays on the line, another member of the licensees' staff can call the NRC Operations Center to verify the authenticity of the call; and (2) The receiver of the original call can hang up the phone and call the NRC Operations Center back to perform the verification. This process is performed similarly if the licensee calls the NRC Operations Center to notify an imminent or actual security threat.

The current verification protocol requires resources that would be better dedicated 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. In light of these issues, NRC will use authentication codes with our licensees to verify a caller's identity whenever a caller notifies an imminent threat. The use of these codes will provide a short, simple means of call authentication that will eliminate the need to perform a call back and still maintain reasonable assurance of the caller's identity.

Proposed Authentication Code Process

On a daily basis, NRC will generate and provide a random 4-digit alphanumeric sequence to each main control room during the daily plant status communications check (4:00 AM). The codes will go into effect each day at 8:00 AM Eastern Standard/Daylight Time (ESDT). In the unlikely event of an imminent threat notification prior to 8:00 AM ESDT, NRC and the licensee

will use the currently in effect code (i.e., the code that NRC-provided the previous day) to authenticate the caller.

NRC has not classified the authentication code as safeguards information. NRC has deemed not classifying the code to be an acceptable risk when balanced by the short lifespan (24 hours) and limited distribution of each daily code and the simplified handling of the information. Although NRC issues only one code at a time, not in sets of a week's or month's worth, NRC still will distribute the authentication code to licensee staff on a "need-to-know" basis to minimize the possibility of caller deception or call "spoofing."

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 picks up the phone, the HOO will indicate the origin and purpose of the call and state that the HOO is ready to authenticate.

3. The licensee will respond when ready for authentication.

4. The HOO then will provide the current authentication code.

5. The licensee will verify that the correct code was given.

6. If the correct code was given, the HOO can pass the information to the licensee without further verification.

7. If the incorrect code was given, the licensee will call back the NRC. 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 NORAD on the line with potential threat information, I am ready to authenticate."

Licensee: "Go ahead NRC."

NRC HOO: "The authentication code is Charlie November Eight Zulu."

Licensee: "That is correct. 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 (DHS)).

Implementation of Authentication Code Process

NRC expects to have this process in place 3 months (12 weeks) after the issuance of this advisory notice. Licensees are responsible for developing procedures and training 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 during the implementation period. These calls will ensure that the process is working and efficient prior to full-scale implementation.

Paperwork Reduction Act Statement: The information collections contained in this Safeguards Advisory are covered by the requirements of 10 CFR Part 50, which were approved by the Office of Management and Budget, approval number 3150-0011.

Public Protection Notification

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 _____

William F. Kane
Deputy Executive Director for Reactor
and Preparedness Programs
Office of the Executive Director