FENOC
FirstEnergy Nuclear Operating Company

Perry Nuclear Power Station
10 Center Road
Perry, Ohio 44081

Mark B. Bezilla
Vice President

440-280-5382
Fax: 440-280-8029

SECURITY-RELATED INFORMATION
WITHHOLD UNDER 10 CFR 2.390

August 14, 2008
L-08-254

10 CFR 50.54(f)

ATTN: Document Control Desk
U. S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT:
Perry Nuclear Power Plant, Unit No. 1
Docket No. 50-440, License No. NPF-58
Response to Request for Additional Information Regarding
Bulletin 2007-01, "Security Officer Attentiveness" (TAC No. MD7635)

In a letter dated December 12, 2007, the Nuclear Regulatory Commission (NRC) issued Bulletin 2007-01, "Security Officer Attentiveness." The FirstEnergy Nuclear Operating Company (FENOC) response for the Perry Nuclear Power Plant (PNPP) was provided on February 11, 2008. On July 3, 2008, the NRC issued a request for additional information (RAI) to FENOC regarding the PNPP response.

Attachments 1 and 2 provide the FENOC response to this RAI. Attachment 2 contains security-related sensitive information and should be withheld from public disclosure under 10 CFR 2.390. Attachment 3 provides a correction to the February 11, 2008 submittal which, since it contains security-related sensitive information, should also be withheld from public disclosure under 10 CFR 2.390. When separated from Attachments 2 and 3, the cover letter and Attachment 1 may be handled as uncontrolled.

A132
NRR

There are no regulatory commitments contained in this letter. If there are any questions, or if additional information is required, please contact Mr. Thomas A. Lentz, Manager – Fleet Licensing, at (330) 761-6071.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 14, 2008.

Sincerely,

Mark B. Bezilla

Attachments:
1. Response to Request for Additional Information, Bulletin 2007-01, "Security Officer Attentiveness"
2. Response to Request for Additional Information, Bulletin 2007-01, "Security Officer Attentiveness" (Security-Related - Withhold Under 10 CFR 2.390)
3. Correction to Information Contained in Response to Bulletin 2007-01, "Security Officer Attentiveness" (Security-Related - Withhold Under 10 CFR 2.390)

cc: NRC Region III Administrator
NRC Resident Inspector
NRR Project Manager

To complete their review, the Nuclear Regulatory Commission (NRC) staff has requested additional information regarding the response to NRC Bulletin 2007-01, "Security Officer Attentiveness." The FirstEnergy Nuclear Operating Company (FENOC) response to the portion of this request which does not contain security-related sensitive information is provided below. The NRC questions are listed below in bold, and are followed by the FENOC responses for the Perry Nuclear Power Plant (PNPP).

QUESTION 3

What is the level of involvement from management who do not have direct responsibility for the security program (including executive and corporate management) in conducting behavior observations of security personnel?

Include the following information in your response:

A description of any processes in place for licensee and/or contract management, who work day to day at the site or visit the site on a routine basis from a corporate office or other applicable offsite location, for conducting behavior observations of security personnel while on duty at their assigned posts. Examples should include, but are not limited to, a discussion of random or scheduled observations conducted by licensee and/or contract management such as the Plant Operations Shift Managers or other Plant Operations Shift Supervisors, Plant Maintenance Supervisors (licensee and contractor), or Quality Assurance Supervisors etc. The discussion should include whether these random or scheduled observations are proceduralized and the required or recommended level of licensee and/or contract management involvement.

RESPONSE

The FENOC Behavior Observation Program (BOP) applies to all personnel granted unescorted access (UA) or unescorted access authorization (UAA) to the FENOC protected and/or vital areas; or those assigned to duties in the Technical Support Center/Emergency Operations Facility (TSC/EOF); or those individuals who administer the Fitness for Duty (FFD) Program. The BOP is an awareness program that ensures personnel are trained in techniques related to recognizing behaviors adverse to the safe operation and security of the facility. Integral to the program is management oversight of employee behavior and an annual review by the assigned supervisor. There are no formal provisions in the program for conducting random or scheduled BOP observations.

BOP training is included in Plant Access Training (PAT), as is the arrest reporting program and annual supervisory review. This training is in accordance with the Unescorted Access Requirements procedure.

The BOP develops observation and recognition skills to satisfy the requirements of both the access authorization (AA) and FFD programs. Personnel are trained in techniques to:

- recognize behaviors adverse to the safe operation and security of the facility,
- observe others in the workplace for aberrant behavior or changes in behavior that might reflect negatively on an individual's trustworthiness or reliability, and
- make appropriate supervisory notifications.

The program also requires that individuals report arrests or other issues that may impair fitness for duty and provides for management oversight of employee behavior with an annual review by the assigned supervisor.

All personnel with unescorted access receive initial BOP training and annual BOP testing in conjunction with PAT. Employees are trained to monitor the behavior of other personnel with unescorted access. BOP monitoring is most effective when conducted by the employees' immediate supervision or management because these individuals are most familiar with normal behavior patterns. All personnel are required to identify and report acts detrimental to public health and safety including security officer inattentiveness.

All supervisors and above at PNPP who have individuals with UAA/UA reporting to them are trained in accordance with the Unescorted Access Requirements procedure. This training is completed prior to being assigned as a supervisor in the Protected Area and Site Security (PASS) system.

FENOC also has an Observation and Coaching program which provides for in-field and training observations, focused observations on specific target areas, and cross-discipline and paired observations. Plant duty week personnel, as well as management personnel from first line supervision through the site operations director, are provided expectations for conducting these observations. Among the trend category examples expected from these observations are job site conditions (which includes environmental conditions) and individual/worker behavior (which includes fitness for duty). The specific areas to be observed are typically selected from scheduled work activities during a duty week. This program provides an opportunity for observation contact time by management personnel from cross-discipline areas.

At PNPP there are no random or scheduled behavior observations specifically designed for personnel outside of the security unit to monitor security personnel. The focus of behavioral observations is the supervisor's observation of direct reports. That supervisor would be most familiar with the behaviors exhibited by direct reports, and would be more likely to make an informed judgment of the exhibited behavior.

Although there is no random scheduled behavior observation specifically designed to monitor security personnel, the scope of the BOP business practice applies to all personnel with unescorted access, who are trained in the behavior observation program. Logically, all personnel holding UA or UAA could monitor security officers. In PAT, personnel are tested to behavioral observation questions. Therefore, personnel are familiar with the program and understand their responsibility to report aberrant behavior.

QUESTION 4

Are security personnel provided opportunities to participate in any personnel surveys regarding the work environment? If so, what is the frequency of the surveys, the average participation rate of security personnel as compared to the general site average, and the process for providing feedback and addressing the results from the survey?

RESPONSE

Yes, all FENOC personnel, including security personnel, are provided opportunities to participate in Safety Conscious Work Environment (SCWE) surveys, which are inputs to the Safety Culture Assessment process. The Safety Culture Assessment process requires that a complete assessment, including all site sections, is conducted annually. SCWE surveys, as an input to the annual Safety Culture Assessment, have been performed on an annual frequency. The Security participation rate for the 2007 SCWE survey was approximately 80 percent, as compared to the average site participation of approximately 71 percent. In 2005, Security participation was approximately 59 percent compared to average site participation of 79 percent; in 2006 the Security participation was approximately 81 percent compared to site participation of approximately 84 percent. A recent independent assessment of the PNPP safety culture and SCWE showed a Security participation rate of approximately 48 percent compared to a site participation average of approximately 80 percent. This recent change in the security participation rate has been documented in the CAP.

The results of the Safety Culture Assessments are reported to the site management team and FENOC executive management, and retained similar to a self-assessment (i.e., available on the FENOC internal network). The assessment results are reviewed

on a quarterly basis as part of the Safety Culture Monitoring process. The overall SCWE survey results are typically provided to the site and fleet leadership teams, and the site managers are typically provided the specific results and comments for their respective sections. The results of the surveys are usually communicated at a summary level via company newsletters, with more detail provided at section or unit meetings following a supervisory briefing. The Safety Culture Assessment process ensures areas requiring prompt or immediate management action are addressed through the Corrective Action Program.

QUESTION 5

How is the licensee's policy regarding site employee attentiveness and/or inattentiveness communicated to personnel, both licensee and contractor, and at what frequency?

RESPONSE

The expectations regarding employee attentiveness and/or inattentiveness are communicated to personnel during annual Plant Access Training (PAT). PAT requalification is provided on an annual basis. This training is provided to all personnel, both licensee and contractor, holding unescorted access or attempting to gain unescorted access. This training reinforces aspects of the BOP including attentiveness issues such as recognizing the signs of fatigue.

At PNPP a post order was created for Security Operations Unit personnel. It provides management expectation for the attentiveness of an officer. This same post order provides some suggested actions appropriate for an officer to remain alert. The post order also provides for the types of approved external stimuli appropriate for the post.

QUESTION 6

Describe the process for employees to file reports through the site corrective action program (CAP). Can employees file CAP reports without prior supervisory/management review or approval?

Include the following information in your response:

Describe the process for employees to file reports through the CAP. Discuss the supervisor/management review and/or approval process including, but not limited to: (1) does a supervisor/manager have the authority to reject a report before entering it into the corrective action program without additional management review and approval; and (2) does a supervisor/manager have the authority to modify the report before such report has been entered into the CAP.

RESPONSE

Every individual involved in FENOC work activities is responsible for using the FENOC Corrective Action Program Condition Report (CR) process to identify conditions, deficiencies and issues that do not meet expectations. Employees can enter condition reports any time directly into the database, from any computer that is connected to the site network. In addition, the Corrective Action Program, defines an Adverse Condition as

> [a]ny event, defect, characteristic, state or activity that prohibits or detracts from safe, efficient nuclear plant operation or a condition that could credibly impact nuclear safety, personnel safety, plant reliability or non-compliance with federal, state, or local regulations.
>
> Adverse Conditions that are failures, malfunctions, deficiencies, deviations, defective hardware and non-conformances, or human performance, programmatic, organizational, or management weaknesses that adversely affect Quality (Q), Augmented Quality (AQ), or nuclear safety related equipment, programs, or processes, are considered conditions adverse to quality.
>
> Adverse Conditions include conditions adverse to quality, plant reliability issues, any concern that should be trended (e.g., personnel contamination, personnel safety, and unexpected plant equipment failures), and conditions that have significance within a regulatory context.

The CAP also requires every individual involved in FENOC work activities, including contractors and vendors, to use the Condition Report process to identify Adverse Conditions and prevents the original described condition in the condition report from being altered without the authorization of the originator.

Employees are encouraged to raise concerns through the CAP as the normal problem resolution process. Should employees wish to raise concerns anonymously, the Employee Concerns Program provides an alternative mechanism to have their concerns evaluated and corrected independently of the normal FENOC problem resolution processes. A review of the generated condition reports is performed by management as a requirement of the CAP and a review of the report's content is performed to ensure information of a sensitive nature is not included. Supervisors do not have the authority or capability to reject or modify a report that has been entered into the CAP.

The CAP process is initiated when any individual identifying an Adverse Condition documents the issue, observation, or concern, by completing the "Originator" section on a CR. Separate CRs are encouraged for each identified issue to help ensure the response is properly focused and to facilitate trending. When conducting maintenance

or troubleshooting on equipment with a documented deficiency, a new individual CR is generated for each newly discovered condition that is not directly related to the original documented deficiency.

When initiating a CR, the originator should clearly describe the problem, including the what, where, when, how, and why, if they are known. The amount of detail in the description should clearly identify the originator's intent in initiating the CR. If the originator has knowledge of the actual or potential consequences of the condition, the description should include a discussion of the consequences. Originators can be contacted during the cause analysis as necessary, and feedback is provided upon completion of the evaluation for CRs they initiate.

Supervisory reviews are expected to take place immediately for reportability, operability, plant or personnel safety issues, and normally within one business day of CR initiation for all other issues. Upon notification by the CR Originator, the supervisor performing initial CR review shall ensure the designated on-shift Senior Reactor Operator (SRO) at the affected site is immediately verbally notified of any Adverse Condition that has any potential impact to plant operations, equipment operability or functionality, plant safety, or personnel safety, or is a potentially reportable condition.

QUESTION 7

Can the employees view the status and disposition of reports directly, or must this information be requested? If yes, please describe the process.

RESPONSE

Yes. The CAP database is accessible from most computers on the FENOC network, and employees only need a network logon password for access to the network to view the status (e.g. review completed and approved) and disposition of condition reports at any time, using the CAP database. The only exceptions are for evaluations that include Safeguards Information or other confidential information. These are maintained in accordance with the appropriate program requirements and may be viewed upon request.

QUESTION 8

Are formal assessments of the security program conducted by organizations/individuals that do not have direct responsibility for the security program? If so, provide information on the process, including, but not limited to, the organizations and levels of management involved, the frequency of such activities, and any tracking of how findings are resolved.

RESPONSE

Formal assessments of the security program are conducted by organizations/individuals independent of both security program management and personnel, such as Fleet Oversight. These organizations/individuals do not have a direct responsibility for implementation of the security program. The security program is reviewed 12 months following initial implementation and at least every 24 months thereafter. The security program review includes:

- an audit of the security procedures and practices,
- an evaluation of the effectiveness of the physical protection program,
- an audit of the Access Authorization and Fitness-For-Duty program,
- an audit of the physical protection system testing and maintenance program, and
- an audit of liaisons established for response by local law enforcement authorities.

A review is conducted as necessary based on assessments or as soon as reasonably practicable, but in no case longer than 12 months, after a change occurs in personnel, procedures, equipment, or facilities that could adversely affect security. The results and recommendations of the security program review, the auditing organization's findings on whether the security program is currently effective, and any actions taken as a result of recommendations from program reviews, are documented in a report to responsible management of both the audited and auditing organization, including the Site Leadership Team (at all sites if a multi-site audit). Findings from the audits are entered into the CAP.

QUESTION 9

How are self-assessment findings and relevant operating experience information communicated to the security force? Describe those processes including, but not limited to, information such as the criteria by which such information is identified, the frequency of such communications, the responsible department(s) or position(s) for such communications, and the recipients of such communications.

Include the following information in your responses:

Describe the process including, but not limited to: (1) formal or informal communication methods; (2) procedures that ensure availability of the policy to staff; and, (3) training opportunities for staff to read and understand the policy.

RESPONSE

Self-assessments are conducted and completed within the FENOC Fleet guidelines established in the FENOC Self-Assessment/Benchmarking business practice. The purpose of this business practice is to establish a consistent process for the preparation, performance, and reporting of self-assessment and benchmarking activities.

The goal of the FENOC Self-Assessment/Benchmarking process is to improve performance in nuclear safety and personnel safety along with the ability to identify gaps and opportunities for improvement. This business practice applies to the performance of all FENOC self-assessment and benchmarking activities.

The FENOC Self-Assessment/Benchmarking process establishes the expectation that FENOC sections conduct self-assessment and benchmarking activities that compare FENOC performance to management expectations, other high performing organizations, industry standards of excellence, and regulatory requirements as a means to facilitate continuous performance improvement.

FENOC sections are expected to frequently compare FENOC performance to industry peers by participating in activities such as visits at other sites, industry conferences, seminars, workshops, and surveys.

FENOC sections should also encourage the participation of industry peers and experts in reviewing FENOC performance and programs, and that FENOC employees participate as team members on assessments and evaluations at other FENOC and industry sites.

Each FENOC Program Manager works with site peers to develop a forecast of the fleet focused self-assessment and focused benchmarking to be performed during the following year. The forecast contains:

- Self-assessment/benchmarking topic
- Projected performance dates
- Report due date
- Team Leader (at least lead plant)
- Sponsoring Director/Manager
- Name(s) of internal peers
- A description of the value added for each self-assessment/ benchmarking activity

The Fleet Corrective Action Program Manager develops an Integrated Assessment Schedule which lists the fleet and site focused self-assessment activities to be performed during the upcoming calendar year from the forecasts provided by the Fleet Program Managers and the Site Regulatory Compliance Managers.

Changes to the established Integrated Assessment Schedule require the concurrence of the Fleet Self-Assessment Review Board (FSARB). This includes any additions, cancellations, and changes in scope, as well as changes in dates. The sponsoring director/manager obtains FSARB members' concurrence for required changes to the Integrated Assessment Schedule.

The self-assessment results are communicated to the appropriate personnel in the affected organizations. Results are reviewed by (or shared with):

- The Section Manager(s) being assessed
- Core Common Process Owner when common processes are assessed
- The groups being evaluated
- Other groups consistent with FENOC practice - for example, relevant Strengths or Noteworthy Items should be shared with selected groups to improve performance.

Strengths and any lessons learned are considered as potential internal or external Operating Experience and communicated with peer groups.

The site team sponsor reports completed focused self-assessment results at the site's Monthly Performance Review (MPR) meeting.

Managers are responsible for ensuring that feedback concerning performance issues, corrective actions and learning information identified is shared with affected and/or interested individuals. The following are some of the methods that are used:

- Individual or group meetings
- Special site announcements
- Performance Indicators
- Site Internet Communications
- Applicable Training Setting

The Security Operating Experience (SOE) Guideline business practice provides the instructions for implementation of the FENOC Security Homeland Security Information Network (HSIN) Operating Experience (OE) Program. The FENOC business practice establishes the guidance for review, analysis and dissemination of security specific HSIN OE through the use of the HSIN database. The primary objective of this program is to ensure that lessons learned are communicated to appropriate personnel and translated into actions to improve the safety and reliability of FENOC Security.

The Executive Leadership Team is responsible for establishing a culture in which OE information is considered beneficial and a vital component for top performance in all areas of plant operation. This responsibility includes ensuring that the proper level of

financial, human and information management resources are provided to effectively implement the OE Program.

The Fleet Security Program Manager ensures a Security Operating Experience Program is established and guidance is in place describing how SOE information is screened, disseminated, evaluated, and documented and the SOE program at each site is implemented and maintained according to this document.

The OE review process determines the level of review required for OE information (e.g., Information Only Review, Evaluation Required). SOE items are entered into the Activity Tracking database. These documents are reviewed for applicability to FENOC Security based on the potential for a similar event or problem occurring within FENOC Security, as well as the possible consequences if a similar event or problem did occur.

If at any time during the OE review or evaluation process an adverse condition is identified as defined in the Corrective Action Program, a Condition Report shall be issued.

The HSIN Security Operating Experience Database (SOED) is used to report all security related OE to the industry. The reporting of SOE is designed to identify critical security event information, site contact information, and appropriate applicable security areas to support SOED search capabilities.

A detailed issue description including cause, corrective action, and safety/security significance is provided. The level of detail contained should be sufficient to provide other industry peers with a complete understanding of the event and actions taken. The level of detail contained in the report may be restricted due to potential Safeguards Information restrictions; in which case, the description should identify that additional critical event information should be collected from the identified site contact using the applicable Safeguards Control processes.

The incorporation of Security Operating Experience into daily work activities is important to the success of the program. Multiple methods to disseminate SOE information to FENOC Security personnel are utilized. Examples of these methods include:

- FENOC Security ensures applicable SOE information is provided as part of the pre-job brief and/or shift turnovers for work activities.
- Direct distribution of SOE information.
- Periodic distribution of summary level SOE information.
- Use of Fleet/Site newsletters.
- Presentation and review in applicable training sessions.
- Recognition of examples of effective use of SOE that improve job performance or prevent errors within Security.

QUESTION 10

How do you assess the effectiveness of your oversight of contractors and subcontractors?

Include the following information in your response:

Describe the licensees' program for oversight of contractors and subcontractors including, but not limited to: (1) a brief overview and description of licensee's procedures that describe the oversight process; (2) include a detailed list (bulleted is preferred) of assigned duties for the licensee supervisor(s) or manager(s) responsible for overseeing contractors and subcontractors at the site; (3) include a detailed list (bulleted is preferred) of the assigned duties for the contractor and subcontractor supervisor(s) or manager(s) responsible for overseeing the contractor and subcontractor staff at the site; and (4) a brief discussion of the corporate (management) involvement with the oversight of contractors and subcontractors at the site.

RESPONSE

Management and oversight of contractors includes the process of identifying, selecting, training, qualifying, supervising, monitoring and assessing contractors. INPO document INPO AP-930, "Supplemental Personnel Process Description," was used as a template for the development of the controlling business practice. FENOC management has established and implemented this business practice to be applied to work activities performed by contractor personnel. It applies to project and work activities at all FENOC facilities. Typically, work activities may include modifications, major maintenance, refueling services and new construction. The requirements apply to both outage and non-outage activities.

Subject matter addressed within the document includes:

- Management expectations for contractors
- Selection of work
- Field oversight process
- Types of contracts
- Requisitioning and award of contracted services
- Contracted worker training and in-processing
- Labor management

- Contract management
- Performance evaluation / feedback

The FENOC line management team always retains ultimate responsibility for ensuring nuclear safety and cannot delegate this responsibility to supplemental contract personnel. Other duties of licensee supervisors or managers responsible for contractor or subcontractor oversight include managing the application of the following processes and programs to the licensee/contractor relationship:

- Safety Overview
- Safety Conscious Work Environment
- Conduct of Maintenance
- Human Performance tools
- Work Management
- ALARA Plan
- Industry Events/Operating experiences
- Construction Labor
- Purchasing Process
- Budget/Cost Control
- In-Processing and Security
- Training
- Field Oversight
- Claims and Delay Management
- Leadership Attributes

Assigned duties for the contractor and subcontractor supervisor(s) or manager(s) responsible for overseeing the contractor and subcontractor staff at the site include managing the application of the following processes and programs:

- Safety Overview
- Safety Conscious Work Environment
- Conduct of Maintenance
- Human Performance tools
- Work Management
- Budget/Cost Control
- In-Processing and Security
- Training
- Industry Events/Operating Experiences
- Procedure Training

Upon completion of the contracted work, FENOC performs an evaluation to assess how well the contractor performed. SCWE and FFD are two of the criteria that are

addressed in this performance evaluation. A post-job meeting is held with the contractor to discuss key lessons learned, strengths, and areas for improvement. The performance evaluations are shared among all FENOC facilities.

Fleet Oversight assesses the effectiveness of the oversight of contractors through performance of the FENOC Work Management assessment audit. Contractors are audited during the compliance audit of Work Management under the audit element of "Control and Oversight of Contracted Services." Self assessments within the Work Management section also provide information used to determine program effectiveness. Negative trends identified are addressed in the CAP.