August 7, 1998

MEMORANDUM TO: Samuel J. Collins, Dierector
Office of Nuclear Reactor Regulation

FROM: David N. Orrik, Capt USN (Ret),
Security Specialist, NRR/DRPM/PSGB

SUBJECT: DIFFERING PROFESSIONAL VIEW REGARDING NRC ABANDONING ITS ONLY COUNTER-TERRORISM PROGRAM.

This Differing Professional View pertains to the NRC's's plan to eliminate Operational Safeguards Response Evaluations and Regional Assists, as currently described in the NRC Inspection Manual as, respectively, procedures 81110 and 81700.

SUMMARY: The United States Nuclear Regulatory Commission has had a security program since 1991 focused on the ability of nuclear power plant security forces to protect against a terrorist attack aimed at causing radiological sabotage, with equivalent consequences of Chernobyl. The heart of this program is security force demonstrations of their armed response capability in onsite force-on-force exercises. Weaknesses were identified in 47% of the plants evaluated to date. There is no other NRC counter-terrorism inspection or oversight effort. The NRC is canceling this program September 30, 1998. This action is ill-advised. The government and the public have placed a high priority on countering the perceived increasing threat of terrorism on U.S. soil. Nuclear plants are a key part of the American infrastructure. The nuclear power industry continues to demonstrate an inability to prepare to protect their plants without NRC oversight/pressure, i.e., "self-regulation" is a failure in plant protection.

1. THE PROBLEM:

a. Protecting against violent assault:

NRC has only one - small - program to ensure that the 60+ nuclear power plants are able to protect against a terrorist attack aimed at causing radiological sabotage, i.e, an "American Chernobyl". The program tests and evaluates their armed response force to respond to a specific threat capability, regardless of its likelihood. The threat capability is specified in 10 CFR 73.1(I), which defines a design basis threat for radiological sabotage. Essentially, it is a small group of well-trained, well-equipped (weapons, explosives, etc.), dedicated terrorists with insider knowledge/assistance making a "determined violent external assault..."

This program is now scheduled to be eliminated on September 30, 1998 (end of FY98).

b. Protecting against attack by stealth:

This same program also assists NRC regional inspections by performing a second type of performance evaluation (of perimeter detection and access control equipment) to ensure that nuclear power plants can protect against one or more individuals attempting to surreptitiously penetrate into the plant in order to cause radiological sabotage. This "attack by stealth" is also part of the design basis threat (10CFR73.1(I)).

This part of the program is now scheduled to be eliminated on September 30, 1999 (end of FY99

c. Implications for USG policy and public upset:

There has been, and will be, no formal announcement or notification of any kind to anyone. An internal-NRC program will just end. However, this action puts the USNRC in the unique position of being the only government agency to end its active involvement in counter-terrorism when both the executive and legislative branches of the government are increasing the emphasis (and funding) for counter-terrorism for (other) government agencies.

Also, the public, when advised, could perceive this as the NRC placing private profit before public and environmental health & safety.

2. THE COUNTER-TERRORISM PROGRAM:

This program is small, employing 3 NRC headquarters personnel (out of 3000 total NRC), assisted by contractors at a cost of $90K/year. The program consists primarily of onsite performance evaluations of a plant's security force and equipment. The heart of these evaluations, called Operational Safeguards Response Evaluations (OSREs), are onsite force-on-force (FOF) exercises with mock terrorists attacking the plant. The "terrorist" force in these exercises varies from a single amateurish individual to a team with the capabilities of the NRC design basis threat. The typical exercise lasts only a few minutes; either the mock terrorists have reached all of their target equipment or they have been interdicted by armed responders who have deployed to key defensive positions with appropriate weapons. This program is almost identical to the one used by DOE for its facilities, except that the NRC was on a much slower frequency, i.e. an OSRE once every 7 years. The contractors, who assist both NRC and DOE, are exceptionally well qualified and trained for this program's efforts.

The second type of performance evaluation, called Regional Assists, conducted by the OSRE team is to physically test the perimeter barriers and alarm systems, CCTV alarm assessment systems, and access control equipment (i.e, X-ray and metal detectors). By jumping, crawling, climbing, etc. the team attempts to defeat the alarm systems and make undetected penetrations into the plant. (Note: Plant personnel are always present so the tests are not confused with actual alarms.) Both individual (i.e., the "lone wolf" terrorist) and team penetration methods are used. This effort also is almost identical to the one used by the DOE for its facilities.

3. PLANT PROTECTION CAPABILITY - AS DEMONSTRATED -:

The evidence over the last seven years from 55 OSREs is that, prior to preparing for an OSRE,

plants would not have been able to demonstrate an assured ability to protect their plant against a terrorist attack. They were unprepared. Why? Regulations do not require nuclear power plants to conduct onsite contingency exercises. (However, category I fuel facilities are required by regulation to conduct contingency exercises onsite and, at least once a year, for observation by NRC.)

In preparing for their OSRE, ALL plants: conducted a vulnerability analysis; developed a new protective strategy; trained trainers; gave new training to their largely inexperienced, civilian guard force in response weapons and tactics; exercised all 3, 4, or 5 shifts in onsite FOF exercises in the new strategy and tactics; added new delay or denial barriers in intruders' likely paths, and added protected/ballistic defensive positions for responding officers. The estimated real cost to a plant, most of it one-time capital expenditures for delay/protection modifications, has been $140k to $800k.

Further, 52 of 55 plants determined in their pre-OSRE work-up that they needed an average of 80% more armed responders than they had committed to in their security plan if they were to "pass" the OSRE. Only when they had to demonstrate their protection capability to the NRC did they arrive at a realistic number based on real performance data. Only one plant had to hire additional security officers; the other plants just assigned response duties to more officers already on shift and then train them.

However, despite 6-12 months advance scheduling, an unvarying design basis threat and list of test-events, and much, intense preparation, 26 of 55 (47%) plants still demonstrated significant protection weaknesses during their OSRE. Further, seven plants had such egregious weaknesses that a return OSRE was scheduled to test the corrective measures. Examples of these weaknesses are when a plant's response force failed to interdict the mock terrorists in all of the onsite exercises, or when a mock-terrorist "success-scenario" is predictable. (Six of these plants have since satisfactorily corrected their weaknesses; the seventh will be retested in August.)

After an OSRE, all plants have relaxed their training/exercising program from the pre-OSRE period. This has meant, in some cases, the end of any formal training or exercising program, no onsite exercises, little or no FOF exercises (which normally requires additional, overtime personnel, e.g., "shadow" shift and exercise controllers), reduction of response team size (to the plan-commitment level), and assignment of response officers to other duties (e.g., fire watch) preventing those officers from being able to meet their response "time-lines".

Additionally, in thirty-six Regional Assists, the OSRE team has identified 117 perimeter intrusion detection sensor weaknesses by physical testing. The team limits testing to the capabilities ascribed to the NRC design basis threat. The team couples this with knowledge of the sensor systems to devise and execute plausible penetration methods. However, in many cases the penetration method, the weakness, lies beyond the plan commitment.

4. OTHER NRC SECURITY EFFORTS:

These two evaluations are the only NRC security evaluations that are performance based. They were begun in 1991 to focus on the armed response and perimeter protection weaknesses being identified in Regulatory Effectiveness Reviews (RERs), which evaluated the effectiveness of safeguards programs, determining if security regulations, as translated into security plans, were effective. The RERs identified 644 weaknesses; the majority were beyond plan commitments and had, therefore, never been previously identified. All were corrected.

The other, current security inspections are regionally based and evaluate a plants' compliance with its security plan, not if the plan works. The OSRE program's benchmark is the NRC's design basis threat. Only the OSRE program physically tests the functioning of the plants total program's ability to protect against the threat. The regional inspectors are, in fact, neither authorized, nor trained, nor physically qualified to do this kind of testing. NRC regional inspectors cannot require or enforce correction of any observed weakness that is beyond commitments in the security plan. However, there has been no correlation between a plant's OSRE performance and either (1) its compliance with commitments in its security plan or, (2) its periodic security quality ratings by NRC, which is derived from, among other things, regional inspection results. In other words, a plant can be in compliance with its security plan and still be unable to protect, with "high assurance", against the design basis threat.

This lack of correlation can become critical. In only 2 plants, of the 26 plants that had response weaknesses identified in an OSRE, were plan violations an issue. In one recent Regional Assist, the perimeter alarm system was penetrated without alarming in 8 places, but in 6 of those locations the penetration method was beyond plan commitments. This was not unusual. NRC inspectors cannot enforce correction of weaknesses that are beyond plan commitments. Further, a plant can reduce its response force to its (minimum) plan commitment with impunity since that reduced number is in the NRC-approved plan. However, the OSRE routinely has caused corrections to be made to weaknesses that appear beyond plan commitments. Of course, the weaknesses are demonstrated; they were real, significant, and obvious, once identified. Only 3 plants have ever challenged RER/OSRE-findings and, for various reasons were unsuccessful. Again, all weaknesses have been corrected.

5. PROGRAM QUALITY;

The OSRE team has consistently received praise from plant/utility management for their professional conduct and the beneficial impact of the OSRE experience on the plant's protection capability. (More specifically, it's been the plants' preparations for the OSRE that has had the salutary impact.) The high quality and impact of the OSRE, and the team, can be verified by questioning the security directors and plant managers of the nuclear power plants that have undergone an OSRE as to their capability before and after the OSRE and the OSRE experience in general.

Additionally, this NRC program has become the model for other government nuclear agencies. Foreign government nuclear officials have observed OSREs or Regional Assists in the last 2-3 years. As a result, parts or all of the program are being copied or used as models in Russia, Kazakstan, Ukraine, Japan, and Germany. At Russia's request, NRC is conducting an OSRE seminar in Russia this August. DOE personnel have also observed an OSRE, and as a result, DOE is planning on devoting one day of its 1999 International Physical Protection Training Course to a presentation of NRC's OSRE and Regional Assist Methodology. Of course, NRC will have canceled it by then. By what criteria will it have been canceled? Cost? Effectiveness? Need in America today?

6. SIGNIFICANCE OF IDENTIFIED WEAKNESSES;

a. Only the capabilities of the NRC design basis threat was used. Therefore, the plants should be able to protect against it. At all times. (Actually, the capabilities used in OSREs are somewhat LESS THAN those specified in 10 CFR 73.1.) The threat has been the same in all OSREs and RERs.
b. Many weaknesses were identified; some were severe.
c. The weaknesses were neiether identified by other NRC inspections nor by the licensees..
d. The weaknesses were predominantly beyond security plan commitments (e.g., in personnel levels and response team exercising).
e. The weaknesses were not identified, or at least not corrected, by the power plants until pre-OSRE preparations. Industry self-regulation failed/is failing.
f. Economic pressure to cut back, reduce personnel (e.g., to plan commitments) is already severe at nuclear power plants. Eliminating the OSRE program will eliminate any countervailing pressure to this economic pressure to reduce plant security forces. Reductions have already been identified by regional inspectors.
g. OSREs have identified some plants where the onsite, FOF exercises indcated that reductions in the actual response team size could be made. The team stipulates only that the plant validate the reductions (with analysis and exercises) and then notify NRC.
h. This program is the ONLY NRC active counter-terrorism effort. It has been effective; plants are correcting significant weaknesses in their protection capability.
i. Armed response weaknesses at power plants regulated by NRC are not new. The GAO identified this in 1977 in a report titled, "Security at Nuclear Powerplants -- At Best, Inadequate." On page ii, the report noted that "...studies conclude that security at nuclear powerplants could not counter sabotage forces of several individuals that were armed and had

knowledge of the plant."

7. IMPACT OF CANCELLATION:

Cancellation of the OSRE program means that 11 plants will not have had an OSRE by the end of FY98. Evidence from the first 55 OSREs is that ONLY those plants that prepare for an OSRE will be prepared to protect the plant against radiological sabotage. Plant security plans have failed to do this. Industry self-regulation has failed to do this. This is as true in 1998 as it was in 1991.
Therefore, to the extent that these plants have not prepared for an OSRE, the evidence is clear that these plants will not be capable of protecting against the design basis threat for radiological sabotage.

Further, security managers admit - volunteer - that, without the specter of a return OSRE visit, they would find it impossible to justify continuing external-threat analysis and shift training to plant/utility management. This is especially true since there is no current regulatory requirement for nuclear power plants (unlike fuel facilities) to exercise their shift response teams onsite, or anywhere. This is a result of utility pressure to reduce costs. Therefore, it is just a matter of time before all or most response forces will have stopped realistic, or any, onsite exercising. Without exercising, the OSRE experience is that these response team's quality will inevitably deteriorate to an inadequate level.

Further, the strong and increasing pressure for nuclear power plants to downsize is especially significant since all plants commit to a specific response force size in their security plans to counter radiological sabotage. (These plans were approved by NRC before the plants went on-line.) However, in 52 of the 55 OSREs, the plants used an average of 80% more responders than they committed to and, therefore, are required -by regulation- to have. The industry's priority has been shown to be, understandably, economic survival then economic profit. Security is a non-productive overhead cost. Plants in all regions are already reducing or planning on reducing security force size, and concomitantly, response force size. Without OSREs (in some form) to evaluate these reductions, to require plants to demonstrate capability with these reduced numbers, NRC will have no recourse but to accept the reduced numbers. This, despite the fact that it was the licensees themselves that determined that they needed the larger number of responders to "pass" an OSRE, whose sole criteria was the NRC design basis threat. Therefore, nuclear power plants will inevitably have an insufficient number of response officers to counter the NRC design basis threat.

It must be emphasized that the NRC design basis threat does not rely on any probabilistic estimate of the likelihood of a "violent external assault." It is a capability, not an intention. Unfortunately, that capability exists - in abundance - overseas and in America. Abandoning this counter-terroist effort will inevitably weaken plant protection to levels unable to protect against the design basis threat capability. "Self-regulation" has clearly failed. It has only been the "threat", i.e., scheduling, of an OSRE that prompted utilities to adequately protect public health and safety. The money they spent preparing for their OSRE in the immediate pre-OSRE period is evidence of this.

There has also been a failure within the NRC to agree upon and ensure that a regulatory basis exists that ensures that power plant licensees (like fuel facilities) can (demonstrably) protect against the NRC design basis threat. It is not an extraordinary capability. Relying on licensee plans, "designed" to protect, has proven unsatisfactory.

David N. Orrik, Capt USN (Ret)

cc:
J. Roe, NRR
R. Rosano, NRR
MModes, RI
GBelisle, RII
JCreed, RIII
BMurray, RIV