April 26, 2016

Michael Layton, Director
Division of Security Operations
Office of Nuclear Security and Incident Response
United States Nuclear Regulatory Commission
Washington, DC 20555

Dear Mr. Layton,

I am writing in reference to the draft memorandum entitled "Recommendations From the Force-on-Force Tactics, Techniques and Procedures Working Group." The draft was made available on public ADAMS on April 14, 2016 (accession number 16105A022).

In light of the growing threat to the U.S. homeland from foreign and domestic extremist groups, the need for the NRC to ensure that licensees are able to protect their facilities against terrorist attacks is more urgent than ever. The NRC's force-on-force (FOF) inspection program is a critical tool in helping to provide the necessary assurance. Consequently, the integrity and rigor of the FOF inspection program must be preserved. A key aspect is the freedom of the NRC's composite adversary force (CAF) to use the full range of tactics, techniques and procedures (TTPs) available to it, consistent with the broad definition of the design basis threat (DBT) as specified in 10 CFR 73.1. The DBT as described in the regulations is the only information available to the public about the characteristics of the adversary that the NRC assumes when assessing the security posture of licensees. Therefore, the NRC has an obligation to meet the public's expectations by ensuring that licensees are able to defend their facilities from adversaries possessing the full spectrum of capabilities described in 10 CFR 73.1.

Implicit in the concept of a "well-trained" adversary (10 CFR 73.1(a)(1)(i)(A)) is the ability to adapt quickly to changing circumstances, to take advantage of opportunities that arise during the course of a mission, and to be innovative. For this reason, when licensee protective strategies are assessed through FOF inspections, it is not only desirable but necessary for mock adversaries to have the leeway to employ novel TTPs and to exploit vulnerabilities in creative ways. Such TTPs should not be viewed as unfair just because they are unfamiliar. If licensees' protective forces are trained to the same standard, they should also be able to respond quickly when new TTPs are used. If they can't, then it is reasonable to question their ability to defend their facilities in the event of a real attack.

In view of the importance of this principle, I have been concerned that the review of TTPs initially ordered by the Commission in SECY-14-0088 could have an inhibitory effect on the range of TTPs used by the CAF, ultimately resulting in an unacceptable decline in the security posture of licensees. However, the Force-on-Force Tactics, Techniques and Procedures Working Group (WG) has alleviated that concern by issuing a number of very sound conclusions and recommendations. I expect that one of the WG's principal findings—that the TTPs used by the NRC CAF during FOF exercises are consistent with the characteristics in the NRC's DBT—will finally put to rest the assertion by the Nuclear Energy Institute (NEI) that the CAF has been using TTPs that are unrealistic and exceed the DBT.[1]

Also important is the WG's finding that all TTPs used by the CAF in NRC-conducted FOF exercises are consistent with demonstrated real-world terrorist training and capabilities, as documented in the Nuclear Intelligence Digest developed by the NRC's Intelligence Liaison and Threat Analysis Branch. It is common sense to interpret the regulatory requirement that the DBT adversary be "well-trained" as commensurate with the level of training routinely being provided overseas today in camps run by sophisticated terrorist organizations. The danger posed to the U.S. homeland by homegrown violent extremists who may covertly receive military training abroad is apparent from the recent testimony of Director of National Intelligence James Clapper.[2]

Another critical finding of the WG is that there are inconsistencies in the quality of the training of mock adversaries and controllers used in licensee-run security drills and exercises, and that this has compromised the ability of some licensees to self-evaluate the effectiveness of their protective strategies and security officer training. This is particularly troubling in light of changes to the Reactor Oversight Process (ROP) and the FOF significance determination process (SDP) over the last several years. These changes give less weight to the results of NRC-run FOF inspections and more weight to baseline security programs, including licensee-run exercises, in assessments of licensee security performance. Moreover, NEI continues to press the NRC to end its own FOF inspections entirely and to rely only on observation of licensee-run exercises.

Given the significant inadequacies outlined by the WG in the conduct of licensee-run drills and exercises, I strongly endorse the WG's recommendation for the development of guidance and criteria to standardize and improve licensee-run programs. Furthermore, credit for licensee-run exercises should only be given if the NRC is able to verify that the exercises have been conducted in accordance with stringent criteria. But even if licensees are able to meet such requirements, there will be a continuing need for independent assessment through NRC-run FOF inspections.

---

[1] Anthony R. Pietrangelo, Nuclear Energy Institute. Request for Closed Commission Meeting on Security. Letter to Stephen G. Burns, Chairman, Nuclear Regulatory Commission. February 25, 2016.

[2] James R. Clapper, Director of National Intelligence. Worldwide Threat Assessment of the U.S. Intelligence Community. Statement for the Record. Senate Armed Services Committee. February 9, 2016.

The only WG recommendation about which I have a reservation is the creation of a formal FOF operational experience information sharing program. A balance must be maintained between allowing sufficient time for the development of effective control measures for new TTPs and ensuring that an element of surprise is preserved in FOF inspections. People will talk. Safeguards need to be in place so that licensee security organizations are not tipped off long in advance that a new TTP may be coming their way, giving them ample time to train to the test.

I hope these preliminary comments are helpful. I look forward to further interactions with your staff on these important matters.

Sincerely,

Edwin S. Lyman, PhD
Senior Scientist
Global Security Program
Union of Concerned Scientists
1825 K St, NW Ste. 800
Washington, DC 20006