INDUSTRY FORCE-ON-FORCE EXERCISE QUESTIONS PROVIDED TO THE NRC SAFEGUARDS STAFF BY NEI FOR DISCUSSION AT THE PUBLIC MEETING ON SEPTEMBER 6, 2000

There have been variations in the conduct of recent OSREs and other NRC security inspections that are leading to confusion in the industry. Many with upcoming evaluations/inspections are concerned that they do not know what to expect and what the criteria will be. In preparation for the staff's September 6, 2000 meeting on future-force-on-force exercises, we request that the staff consider the following areas of confusion raised by the industry. Some questions may be broader or more pointed than the intended staff discussion but are valid in the mind of the submitter and deserve consideration. Although each question does not need to be answered individually, we hope that the overall briefing would clarify the NRC's intent/expectations in each area.

1. What security inspections are currently scheduled? What determining factors are used by the NRC for the scheduling? Why is an OSRE scheduled to take four days to conduct?

2. What inspection guidance will be used for:
   - OSREs?
   - Region Assists?
   - Baseline Inspections?
   - What is the relationship between IP 81110 "Operational Safeguards Response Evaluation (OSRE)," and the baseline inspection program, IP 71130 Attachment 03?
   - Will a licensee's target analysis/methodology continue to be acceptable as per IP 81110, or will use of IP 71130.03 by the Regions preclude this?
   - Will OSREs or "assist visits" be required following major modifications to validate the licensee's changed safeguards systems and/or the protection strategy?

7. Will force-on-force exercises/drills be conducted by the NRC in any security inspections other than the OSREs?

8. We understand responsibility for running the OSREs has been shifted to the regions.
   - What place will headquarters have in the program and what impact is envisioned that this shift will have on the licensee?
   - How will program consistency be maintained across the industry?

5. What elements of tabletop exercises and force-on-force exercise/drills are risk-informed quantitatively and qualitatively?
   - What is the likelihood of an occurrence of an actual radiological sabotage event that considers risk-informed information?
   - What is the process for determining that a radiological sabotage event has or could have occurred based on tabletop exercises or force-on-force exercise/drills?
   - What analytical tools will be employed to validate that damage inflicted by a DBT adversary under a tabletop exercise or force-on-force exercise/drill has in fact resulted in a radiological sabotage event?

4. What is the intent of "target sets" as used in the OSRE program? We note a difference between the intent in IP 81110 and IP 71130.03. The first does not make any assumptions on the bases of a licensee's defensive strategy. The second assumes that the defensive strategy is based on target sets.

5. If a licensee uses target sets as the basis for a protection strategy, what is the purpose of an inspector suggesting changes to the developed target sets?

6. Can the adversary be credited for action that he/she does not take or simulate during the exercise/drill? If some items in a target set are not protected in the strategy, can they be used in mitigation if the adversary does not simulate destroying them?

7. Variations in the approach to credit for operator action have been noted.
   - How is operator action considered during the conduct of an exercise/drill?
   - How is operator action considered during review of the significance of exercise/drill deficiencies?
   - Are all security barriers, delay devices, and security defensive aids required to be included in the Physical Security Plan (PSP) before credit is given?
   - Why do some inspectors require that that any SSC that would be used in operator mitigation would have to have been included in a target set?
   - What is the current NRC performance position in grading an exercise/drill? If four out of five SSCs in a postulated target set are neutralized by an adversary such that significant core damage would not be an outcome and the public health and safety were protected, would that be a satisfactory outcome for the exercise? If not, why?

- Since most OSRE events are characterized as "beyond the design basis events" as specified in the Updated Final Safety Analysis Reports, what is the regulatory basis for not crediting operator action to mitigate safeguards events similar to how any other non-safeguards event would be mitigated?

7. Is it true that the current security Significance Determination Process (SDP) is being reviewed and currently being held in abeyance for OSRE findings because it over predicts items with respect to safety significance? If so, how will the staff evaluate exercises/drills while the SDP is being modified? Will the revised SDP contain performance criteria to be used for significance determination?

8. When will the licensee be provided current capabilities to be considered in establishing an adversary force for a DBT level exercise, i.e., when will licensees be provided with a written OSRE adversary characteristic description (safeguards document)?

9. What is the justification for an OSRE inspection team to evaluate exercise/drill performance assuming that no operator response outside of Control Room is possible until all adversaries have been eliminated? Please explain the “other damage control resources” and SDP review that the staff has requested during recent OSREs? Why is that being requested? Does it restrict a plant’s response during an exercise/drill?

10. What industrial safety considerations (i.e., running unguarded roof lines, climbing unsecured ladders, running with loose equipment through Spent Fuel Pool area, etc.) are expected for scenarios proposed by OSRE inspection teams included adversary actions deemed unacceptable from a safety standpoint? OSHA requirements implemented by licensee safety organizations prevent operating/testing the way the OSRE does.

11. The OSRE team provides information not normally available to an attacking force.
    - What authorizes the OSRE team to probe the defensive strategy through discovery during tabletop and force-on-force exercises/drills?
    - Where/how could an adversary obtain such a level of intelligence?
    - In preparation for conducting force-on-force exercise/drills, why should the adversaries be provided with the complete contingency response strategy (including tours of defensive positions, detailed knowledge gained through tabletops and interviews with security trainers and response team personnel) that is then exploited?

- Purportedly, defense in depth is evaluated by tabletops being continued beyond adversary failure. Is this the only purpose or is it a tool for exploitation by a knowledgeable adversary?
- Why does the OSRE team try to multiply a success (learned potential vulnerability) by exploiting it during a follow-on similar exercise? This would be the equivalent of the adversary launching multiple attacks (the DBT postulates only a single attack) and adjusting the battle plan dependent upon the defender's previous response. Wouldn't it be more appropriate to obtain other lessons/goals with a different exercise scenario?
- How can an exercise/drill implementation "artificiality" be taken into consideration in determining exercise outcomes?
- In order to avoid subjective conclusions/challenges of perception between the OSRE team and the licensee, why not require a formal attack plan by the adversary to be available in the critique to determine who was successful in meeting goals?
- Since actual adversaries would have to go through the owner-controlled area, why is there no allowance for licensee personnel's ability to alert security of noted adversary activities prior to PA penetration?

4. If the requirements and performance criteria are detailed in the procedure, why can't an OSRE evaluation team conduct a final exit prior to the NRC team's departure from the site?

5. When and how should the intrusion detection system (IDS) "challenge testing" be conducted — during an OSRE, Attachment 3 Inspection, Region Assist, or other?

   - Why the extensive IDS challenge testing per 71130.03 when the Regional inspector already does this on each inspection visit to the site?
   - Why should the inspection team be allowed to probe several places? How many attempts to penetrate an IDS are allowed prior to declaring a system defeat, i.e., multiple intrusion attempts at the same location would not be possible for an actual adversary?
   - What if the test is done outside of the requirements of the security plan and beyond the manufacturer's limits? What is the time limit for crawl testing of IDS while under direct observation of security personnel, i.e., taking extensive time to set up for testing without giving credit for CCTV coverage of zones, observation by security officers, or other employees to detect adversary penetration?
   - What are the published criteria for NRC jump testing of the IDS?

- Why do the Regional inspectors check IDS junction box tamper switches when this is not part of IP 71130.03?

6. What should the licensee do when that an unrealistic exercise scenario has been proposed?

7. We understand that the NRC has changed its enforcement policy relative to OSRE results. Could you provide a copy of that policy and the supporting rational?

8. What regulatory process will be used to modify the OSRE program and how will licensees be informed of the changes?

9. What will be required to shift from the OSRE program to the industry developed Safeguards Performance Assessment (SPA) Program?

10. Unlike military defense conditions, why require licensee security forces to be on maximum alert continuously with immediate response capability within seconds with no known or perceived threat to a hardened facility like a nuclear power plant? Why doesn't the NRC share with cleared individuals in the industry its intelligence regarding local known/potential adversary situations on a real-time basis? A security alert level posture could be easily implemented.

11. What authorizes NRC contractors to specify the capabilities of various types of explosives and ordinance without providing substantiation? Factors driving this issues include:

    (a) Use of escalated weapons capability. When will the NRC obtain federal authorization for nuclear power plant operators to be armed with equivalent arms/armament currently afforded the DBT adversary?

    (b) Why is it assumed that the adversaries have flawless execution for their explosive successes? Would it not take a technical evaluation of structural design versus actual placement of simulated explosives to properly evaluate anticipated destruction? If the OSRE team will continue to postulate explosive penetration of reinforced concrete walls to gain access to targets, will the NRC provide licensees with the criteria used for determining penetration capabilities? In addition, will the NRC provide licensees with the delay criteria for various barriers & tactics, e.g., cutting/breaching fences, doors, blowing a 24" to 36" reinforced concrete wall, etc.?

(c) Since security force response must be realistic and demonstrate the ability to defend targets, why isn't the adversarial force required to demonstrate proper planning, use and accounting for ammunition and explosives?

(d) If security officers can qualify on the 10 CFR 73.55, App. B, approved course of fire, why must they demonstrate their stress fire accuracy ability for every possible firing position in the plant?

5. Incident to the transfer of responsibility for the conduct of OSREs from the headquarters to the regions, why is an OSRE scheduled regardless of the impact to the licensees, especially when multiple NRC team inspections have already been conducted that same year?

6. Can you provide any written OGC determination about how OSRE findings of vulnerability are enforceable and specifically where in the rule the required performance is a requirement?
   - What is the legal basis for enforcement action concerning undefined weaknesses/vulnerabilities discovered during an OSRE as the result of hypothetical assumptions or inadequate exercise/drill staging, but not based on actual conditions?
   - Why am I not allowed to use trained personnel in OSRE exercises that are on site and can respond in a less than immediate timeline, to engage the adversary or support the response team?
   - As long as a licensee maintains the minimum number of responders required by the rule, what is the regulatory basis for specifying how the contingency response force is constructed?
   - Why restrict the number of responders when in real life all available/trained security officers would be used to mitigate an actual safeguards threat?