

POGO Presentation to NRC Security Inspectors

December 16, 2004

Arlington, Texas

By

Danielle Brian and Peter Stockton

www.pogo.org

pogo@pogo.org

202-347-1122

Two Great Resources

- NRC Headquarters Security leadership, particularly Roy Zimmerman and Glenn Tracy, support efforts to improve security. Bring your concerns to them.
- Plant Security Officers are your eyes and ears, but the allegations process has caused most to have little confidence in the NRC. Good channels of communication between security officers and inspectors is essential.

Allegations Program Pitfalls

- Don't consider the allegation as a disruption. Consider it an opportunity to be resolved.
- Don't focus only on compliance with regulations. Instead focus on whether security is as robust as it should be.
- Don't rely only on licensee's assessment
- Don't rely only on NRC site representative
- Don't rely only on guard union president

Allegations Program Tips

DO:

- take advantage of this opportunity to find out what is REALLY going on at the plant
- talk to numerous security officers
- ask whistleblower to identify people and documents that can prove allegation
- communicate with whistleblower what you are finding (as much as you can)
- tell whistleblower not to tell any of his colleagues that he has made allegation

Why do these Failures in the Allegations Program Matter?

- Huge impact on morale of guard force when NRC and security contractor don't appear to care about security concerns:
 - On retention of security force
 - On commitment to defend the plant under attack

Example: Indian Point consultant found 81% of guards no longer believed plant could be defended under real attack. (Would the guard force stay and fight when under attack?)

What Not to Do:

Case Study on Fitness-for-Duty

- Allegation: Security Officers are “asked” to work 60-70+ hour weeks (not during outage)
- Pre-Fatigue Order Result: NRC finds allegation true, but licensee in compliance with regulations, so issue never raised with NRC Headquarters
- Post Fatigue Order Result: NRC relies on old reviews, doesn't come to plant after allegation is made, tells whistleblower he's wrong, but doesn't tell him why because it's classified

What Not to Do:

Case Study on Bullet Resistant Enclosures

- Allegation: Bullet Resistant Enclosures present vulnerabilities, but classification concerns prevent whistleblower from providing details over phone.
- Result: NRC never talks to whistleblower, and sends letter back saying licensee denies problem. Period.

Things for You to Keep in Mind

- Questionable Security Plans
- Unrealistic Reliance on Outside Responders
- Force-on-Force Artificialities and Cheating
- Inadequate Design Basis Threat

Questionable Security Plans

- How thoroughly tested are site security plans, if 65 plans were approved in six months? It takes the Energy Department that long to get one approved.
- Are plans based on worst case scenario vulnerability analyses that are performance tested, or are they simply compliance driven?

Reliance on Outside Responders: Compliance vs Reality

- NRC regulations only require guard force to hold off attackers until outside SWAT team arrives. If the attackers are enemies of the state, guard forces aren't responsible at all.
- Attacks would likely be over in 3 to 8 minutes, and tests have shown that it generally takes nearly 2 hours for a SWAT team to arrive and provide help.

Force-on-Force Improvements

NRC should be commended for improvements over past year:

- using MILES equipment,
- beginning to use JCATS computer simulations,
- developing dedicated mock adversary team.

However:

Force-on-Force Conflict of Interest

- NRC let Nuclear Energy Institute (NEI) decide adversarial force. NEI hired Wackenhut
- Wackenhut will be testing itself about 50% of the time. The rest of the time, Wackenhut will be testing its competitors.
- Even if guard force is successful in repelling mock attack, there will be little public trust in the test.

Force-On-Force Artificialities

- **Schedule is known a year in advance, allowing for cramming for weeks prior to test**
- **Wackenhut adversary force trains guards the week before testing them**
- **Energy Dept. movie “Systems Under Fire” exposes weaknesses in previously accepted defenses**
- **MILES Bravery: if 20-40% of force in real life is lost, combat effectiveness is lost, but you can still “win” with those casualty rates in FOF test**
- **Terrorists always have three advantages not tested:**
 - **Surprise**
 - **Speed**
 - **Violence of Action (i.e. how will guards react to live fire and casualties?)**

Cheating Can Be Blatant or Subtle

- Cheating at Oak Ridge included tape on sensors and guards knowing location of attacks. It took DOE inspectors a decade to discover this.
- DOE Transportation Division guard force has been caught with copies of attack plans.
- How will the NRC evaluator or controller detect subtle cheating. For example if a mock terrorist is running slower than required?

Inadequate Design Basis Threat

- NRC states DBT “is an adequate and reasonable standard for a private security force to protect against,” not a standard based on the actual threat.
- However, the intelligence community’s Postulated Threat does not differentiate between types of nuclear facilities – threat is same for private power plants and gov’t facilities.
- DOE facilities are required to protect against about three times as many adversaries, as well as a greater array of weapons, than the NRC requires.

You Have an Essential Job

- Terrorists have shown they are targeting nuclear sites
- You are empowered to protect the country from such an attack
- Security forces need you to be responsive to their concerns
- Let the Region/HQ know if you believe a site does not have an adequate security posture, even if it is in compliance