UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Standard for Physical Security	**)**	**Docket No. RM14-15-000**
Request for Rehearing on FERC Order No. 802	**)**	
Filed by the Foundation for Resilient Societies		

REQUEST FOR REHEARING OF FERC ORDER NO. 802 AND REMAND OF RELIABILITY STANDARD FOR PHYSICAL SECURITY, 149 FERC ¶ 61,140 (November 20, 2014)

Submitted to FERC on December 21, 2014[1]

Pursuant to section 313(a) of the Federal Power Act ("FPA"), 16 U.S.C. § 825 (a), and Rule 713 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Rules of Practice and Procedure, 18 C.F.R. § 385.713, the Foundation for Resilient Societies (hereafter "Resilient Societies"[2]) hereby respectfully submits this Request for Rehearing of the Final Rule issued in this Docket and Motion for Remand, relating to FERC Order No. 802, a Reliability Standard for Physical Security.

Resilient Societies is incorporated in the State of New Hampshire as a non-profit organization engaged in scientific research and education with the goal of protecting technologically-advanced societies from infrequently occurring natural and man-made disasters. Resilient Societies seeks a more robust and resilient bulk power system, in part because all other critical infrastructures depend upon the reliability and recovery of the bulk power system. Resilient Societies seeks to identify cost-effective opportunities to protect societies and then develop policy initiatives. Information about Resilient Societies may be found at www.resilientsocieties.org.

[1] The Request for Rehearing is timely filed, because the 30-day filing deadline falls on Saturday December 20, 2014, and the FERC Office of the Secretary advised that filing on Monday, December 22, 2014 would be timely. See also *Cities of Batavia, et al.* v. *FERC*, 672 F.2d 64 at 72 (D.C. Circuit, 1982)(FERC regulations extend filing deadlines for weekend due dates and for legal holidays in the District of Columbia).

[2] We respectfully request that our organization be identified in FERC rulings as "Foundation for Resilient Societies" or "Resilient Societies" instead of the nonspecific identifier "Foundation."

Background

On November 20, 2014 the Commission approved Reliability Standard CIP-014-1 (Physical Security) in FERC Order No. 802. The North American Electric Reliability Corporation, the Commission-certified Electric Reliability Organization, submitted Reliability Standard CIP-014-1 for Commission approval in response to a Commission order issued on March 7, 2014. The purpose of Reliability Standard CIP-014-1 is to enhance physical security measures for the most critical Bulk-Power System facilities and thereby lessen the overall vulnerability of the Bulk-Power System against physical attacks. In addition, the Commission directed NERC to develop one modification to Reliability Standard CIP-014-1 and submit an informational filing.

Pursuant to Section 215 of the Federal Power Act ("Section 215"), the Commission approved Reliability Standard CIP-014-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

The March 7, 2014 Commission Order, "Reliability Standards for Physical Security Measures" Docket No. RD14-6-000, indicated that the Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. Specifically, the March 7 Order directed that the Reliability Standards should require: (1) owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities"; (2) owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities; and (3) those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

In its May 24, 2014 Petition NERC asserted that Reliability Standard CIP-014-1 "serves the vital reliability goal of enhancing physical security measures for the most critical Bulk-Power System facilities and lessening the overall vulnerability of the Bulk-Power System to physical attacks."[3]

[3] NERC Petition at 15-16.

NERC maintains that the "appropriate focus of the proposed Reliability Standard is Transmission stations and Transmission substations, which are uniquely essential elements of the Bulk-Power System."[4] The Reliability Standard is applicable to Transmission Owners that satisfy the Applicability Sections 4.1.1.1, 4.1.1.2, 4.1.1.3, or 4.1.1.4, and to Transmission Operators. NERC states that the transmission facilities covered by Applicability Sections 4.1.1.1 through 4.1.1.4 match the "Medium Impact" transmission facilities listed in Attachment 1 (Impact Rating Criteria), specifically, the "Medium Impact" facilities described in Sections 2.4, 2.5, 2.6, and 2.7, of Reliability Standard CIP-002-5.1.[5]

On November 20, 2014 in FERC Order No. 802, the Commission determined that the Commission's enforcement authority under Federal Power Act Section 215(e), and particularly the use of targeted auditing following implementation of Reliability Standard CIP-014-1, will allow FERC to address the concerns raised in the NOPR. Thus, the Commission excluded from the scope of Physical Security Standards (1) all generator facilities within the Bulk Power System; and (2) three sets of control centers and backup control centers out of the 16 sets of control centers and backup control centers of U.S. Reliability Coordinators, facilities that are owned and operated by other than transmission system owners or operators.

The Commission required an informational filing to address "High Impact" control centers, but within a two year period measured from the date of implementation of Order No. 802 and without any duty to upgrade physical security protections:

> The Commission adopts the proposal to direct NERC to make an informational filing addressing whether Reliability Standard CIP-014-1 provides physical security for all "High Impact" control centers, as that term is defined in Reliability Standard CIP-002-5.1, necessary for the reliable operation of the Bulk-Power System. However, the Commission extends the deadline for that informational filing until two years following the effective date of Reliability Standard CIP-014-1.

[4] *Id.* at 18. NERC states that, although the terms "Transmission stations" and "Transmission substations" are sometimes used interchangeably, Reliability Standard CIP-014-1 uses the term "Transmission substation" to refer to a facility contained within a physical border (e.g., a fence or wall) that contains one or more autotransformers. *Id.* According to NERC, the term "Transmission station," as used in Reliability Standard CIP-014-1, refers to a facility that functions as a switching station or switchyard but does not contain autotransformers. *Id.* at 18-19.
[5] *Id.* at 25 (citing Reliability Standard CIP-002-5.1 (Cyber Security — BES Cyber System Categorization), Attachment 1 (Impact Rating Criteria)).

Moreover, FERC Order No. 802 declined to address the request of Resilient Societies that the reliability standard be modified to require Force-on-Force exercises to validate the efficacy of physical security plans and operations, rather than a set of paper plans for physical security to be validated by peer utility review, or by review by another third party.

Resilient Societies participated in standard-setting at NERC for Reliability Standard CIP-014-1 and submitted comments to the Standard Drafting Team. Resilient Societies later submitted comments in rulemaking under FERC Docket RM14-15-000.[6] Unfortunately, FERC did not address many of the comments submitted by Resilient Societies in rulemaking. FERC's failure to address our comments is the legal basis for this Request for Rehearing.

Statement of Issues and Specifications of Error

1. Arbitrary exclusion of all Generator Operators and failure of FERC to address our comments on how an attack on Generator Operators could cause cascading outage.

Resilient Societies stated in its Comments dated September 8, 2014 and gave further explanation in Appendix 1 of the Comments:

> Reliability Standard CIP-014-1 unreasonably exempts whole categories of NERC Registered Entities that are critical to the reliable operation of the Bulk Power System. These entities include:
>
> 1. Reliability Coordinators (RCs)
> 2. Balancing Authorities
> 3. Generator Operators and Generator Owners
>
> For a detailed rationale for why these entities should be included in the standard's Applicable Entities, see Appendix 1.

Resilient Societies stated in its Comments dated September 8, 2014:

> Approximately 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more—this number is a rough approximation of the number of

[6] See "Comments of the Foundation for Resilient Societies Submitted to FERC on September 8, 2014 and Reply Comments of September 22, 2014" under FERC Docket RM14-15-000, incorporated in their entirety by reference.

> generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked.

Resilient Societies quoted in its Reply Comments dated September 22, 2014 the testimony of FERC Chairman Cheryl LaFleur before the Senate Energy Committee:[7]

> A carefully planned and executed attack on a single or multiple generation plants could cause cascading outages…

None of the above comments of Resilient Societies were addressed in FERC Order No. 802 in Paragraphs 96 to 98 contained in section "F. Generators," or elsewhere in the Order.

For illustrative purposes only, but not as additional facts, we give an example of three generation facilities that might cause cascading outage in Appendix 1 to this filing.

2. For the arbitrary and unsupported time period of at least two years, arbitrary exemption of protection for high impact" control centers and backup control centers for Reliability Coordinators and Balancing Authorities and failure of FERC to address our comments on how a coordinated attack on control centers could cause cascading outage.

Resilient Societies stated in its Comments dated September 8, 2014 and gave further explanation in Appendix 1 of the Comments:

> Reliability Standard CIP-014-1 unreasonably exempts whole categories of NERC Registered Entities that are critical to the reliable operation of the Bulk Power System. These entities include:
>
> 1. Reliability Coordinators (RCs)
> 2. Balancing Authorities
> 3. Generator Operators and Generator Owners
>
> For a detailed rationale for why these entities should be included in the standard's Applicable Entities, see Appendix 1.

[7] Testimony of FERC Chairman Cheryl LaFleur, to U.S. Senate Energy Committee in a letter dated June 4, 2014, available at http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=86e83c32-636a-40b6-8e5d-c072f2f95a8c. See "Question 16: Could an attack on an electric generation plant cause a cascading outage or long term power shortage? Answer: A carefully planned and executed attack on a single or multiple generation plants could cause cascading outages, but I have not seen information that would lead me to believe that it could cause a long-term power shortage. The extent and duration of any outage from an attack would depend upon a number of factors..."

Resilient Societies stated in its Reply Comments dated September 22, 2014:

> Out of 16 Reliability Coordinators, three would be exempted from the standard because they are not also designated in the NERC Compliance Registry as Transmission Operators. These three Reliability Coordinators—Peak Reliability, Midcontinent ISO, and Southwest Power Pool—supervise power for 141 million Americans and Canadians.
>
> The U.S. and Canada already had a cascading outage in 2003 because of inadequate reliability coordination. In particular, in August 2003 the Midwest Independent System Operator (MISO), a Reliability Coordinator, lacked real-time data from First Energy, and lacked broad visibility over 37 control areas. These constraints led to inadequate diagnostic assistance and direction. Mandatory reliability coordination might well have averted a cascading blackout throughout much of the Northeast and Canada.[8]
>
> A concurrent physical attack on a Reliability Coordinator's primary control center and its backup control center can replicate the conditions of August 14, 2003: causing the unavailability of usable real-time data. The Reliability Coordinator would become unable to provide diagnostic assistance and direction to minimize blackout risk and prevent damage to grid-critical equipment. Moreover, under the NERC system of standards, Reliability Coordinators are solely responsible for managing system restoration, so an attack on both transformer substations and Reliability Coordinators could be long-lasting. FERC should not give weight to comments that promote the exemption of Reliability Coordinators.

None of the above comments of Resilient Societies were addressed in FERC Order No. 802 in Paragraphs 53 to 56 contained in section "C. Informational Filing on 'High Impact' Control Centers," or elsewhere in the Order. Instead, FERC arbitrarily exempted NERC from standard-setting for high impact control centers for a period of two years while NERC prepares an "informational filing." FERC gave no justification for the arbitrary time period of two years and as a result the public might reasonably conclude that protection of "high impact" control centers is not important to the reliability and security of the Bulk Power System.

For illustrative purposes only, but not as additional facts, we show in in Appendix 1 to this filing examples of a Reliability Coordinators and Balancing Authorities where a coordinated physical attack that might cause cascading outage and/or system restoration issues.

[8] See "U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," (April 2004) at pp. 18-19, 49-50, 67, 110, 139, and 159-160, available at http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

3. Arbitrary failure to address how system restoration could be conducted when a coordinated attack is executed on Reliability Coordinators and failure of FERC to address our comments on the critical role of Reliability Coordinators under the FERC-approved NERC standard system.

In NERC standard setting and on FERC docket RM14-15-000 we commented:

> Reliability Coordinators (RCs) would be exempted under the draft standard. Not all Reliability Coordinators are Transmission Operators or Owners. Peak Reliability, Midcontinent ISO, and Southwest Power Pool would be exempted because they are not in the NERC Compliance Registry as Transmission Operators or Owners. (MISO is not a Reliability Coordinator under its MRO registration.) The following standards apply to Reliability Coordinators but not Transmission Operators and Owners: Standard EOP-006-2 — "System Restoration Coordination"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies" (Applies to Balancing Authorities, Reliability Coordinators, and Load-Serving Entities); Standard IRO-009-1 — "Reliability Coordinator Actions to Operate Within IROLs"; Standard IRO-015-1 — "Notifications and Information Exchange Between Reliability Coordinators." The Joint U.S.-Canada report on the 2003 Blackout concluded that insufficient wide-area control, such as that provided by Reliability Coordinators, was a contributing factor to the blackout. Yet the Standard Drafting Team has disregarded these findings in exempting Reliability Coordinators. It is a fallacy to believe that only entities with direct control of substations need protection from physical attack. If critical substations and their Reliability Coordinators are attacked in a coordinated manner, what entity will lead system restoration? It is essential that Reliability Coordinators are designated as responsible entities, both to protect their own facilities and to enable their authority to review the adequacy of physical security capabilities for operating utilities in their coordinating areas. Key findings of the joint U.S.- Canada Outage Task Force on the August 2003 blackout demonstrated the need for the Reliability Coordinators to actively supervise operating entities both to meet essential operating needs and to assure adequate regional visibility. See U.S.-Canada Power System Outage Task Force Report (April 2004). <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>

None of the above comments of Resilient Societies were addressed in FERC Order No. 802.

4. Arbitrary exclusion of other facilities within the Bulk Power System that could cause cascading outage if attacked and failure of FERC to address our comments on how an attack on exempted substations could cause cascading outage.

Resilient Societies stated in its Comments dated September 8, 2014 and gave further explanation in Appendix 1 of the Comments:

The standard does not require modeled contingency planning for scenarios of physical attack. Without explicit modeling for physical attack, some substations may fall through the cracks under "Aggregate Weighted Value" methodology in the standard.

Resilient Societies stated in its Reply Comments dated September 22, 2014:

> The Bulk Power System has not been designed for resilience against purposeful physical attack. Instead, the Bulk Power System has been designed for resilience against random electrical and mechanical failure of individual transformers, generation units, control centers, etc. The N-1 planning criterion commonly assumes a single failure, not the simultaneous failure of all transformers at a substation, or all units at a large generation facility, or both a primary and backup control center. In a physical attack by an intelligent, organized adversary, the purpose of the attackers would be to cause multiple failures simultaneously and thereby overwhelm N-1 resilience planning.

The above comments of Resilient Societies were not addressed in FERC Order No. 802 in Paragraphs 39 to 41 contained in section "B. Applicable Governmental Authority's Ability to Add or Subtract Facilities from an Entity's List of Critical Facilities" or elsewhere in the Order.

5. Arbitrary exclusion of specific security measures for critical grid facilities and failure of FERC to address our comments on specific security measures and on "best practices" that would be based upon Force-on-Force exercises.

Resilient Societies stated in its Comments dated September 8, 2014 and gave further explanation in Appendix 1, 2, and 3 of the Comments:

> While FERC Directive RD14-6-000 did not require specific security measures, it could have been reasonably expected that NERC would have developed specific measures to be applied on an as-needed basis. Nonetheless, the draft standard contains no specific requirements or even suggested guidelines for physical security measures. Examples of specific physical security requirements that should be considered include:
>
> - **Gunfire Locators.** Gunfire locators, had they been installed at Metcalf Substation, could have alerted system operators to the attack in real-time, allowing prompt dispatch of law enforcement.
> - **Intentional Electromagnetic Interference (IEMI) Detectors.** IEMI detectors would be another specific security measure that could alert both specific site managers and Bulk Power System operators of hazards that go beyond an attack on a single facility.

- **Automated Intrusion Detection Alarm System Reporting**. Alarms should be reported to Reliability Coordinators, local and state law enforcement, and federal operations centers. One function of effective physical security measures should be to expedite wide-area visibility and reliable rapid response to counter physical attacks before extensive damage is inflicted. We have developed an understanding of the feasibility of automated alarm reporting to multiple recipients – whether the threat is a solar storm or a physical security attack. To avert the concurrent loss of many grid-critical facilities, the automated receipt of near-real-time security alarms could enable: deployment of local law enforcement, state law enforcement, or mobilization of the National Guard.

None of the above comments on specific security measures were addressed in FERC Order No. 802 in Paragraphs 77 to 83 contained in section "E. Third-Party Verification and Review," or in Paragraphs 109 to 111 contained in section "H. Other Issues," or elsewhere in the Order.

Resilient Societies stated in its Reply Comments dated September 22, 2014:

> The concurrent attack on selected generating facilities, perhaps combined with cyber-attacks on control centers and communication networks, could cause widespread and persistent outages. Hence, Resilient Societies recommends that:
>
> 1. FERC exclude NRC-licensed nuclear generating facilities from any listing as "Critical Facilities" to be included in mandatory physical security standards, a modification of CIP-014-1; and
> 2. FERC order modification by NERC of Physical Security Standard CIP-014-1 to include non-NRC-licensed generating facilities with combined facility generating capacity above a Commission and NERC-determined limit, to be designated "Critical Facilities"; and
> 3. FERC by an order to NERC require modifications of Physical Security Standard CIP-014-1 to include Force-on-Force exercises for all designated "Critical Facilities" to validate and assess the adequacy of physical security plans and the adequacy of coordinated responses of facility security personnel, and law enforcement personnel as needed.

None of the above comments on Force-on-Force exercises were addressed in FERC Order No. 802 in Paragraphs 77 to 83 contained in section "E. Third-Party Verification and Review," or in Paragraphs 109 to 111 contained in section "H. Other Issues," or elsewhere in the Order.[9]

6. Cost-effectiveness of physical security protective measures for the Bulk Power System and failure of FERC to consider the cost and benefits of protective measures, including adverse impact on human populations were an attack to occur.

Resilient Societies stated in its Comments dated September 8, 2014

> Improvements to the standard that we suggest would be marginal additions of facilities and their equipment and therefore would be cost-effective. We propose inclusion of primary and backup control centers for Peak Reliability, MISO, and SPP—an increase of 6 control centers as compared to approximately 200 already included Transmission Operator control centers. We propose inclusion of 19 additional Balancing Authorities as compared to 114 Balancing Authorities in total. There are only 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more—this number is a rough approximation of the number of generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked.

A list of 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more is provided in Appendix 1. The three main sources of on-site stockpiled energy supplies for electric generation are nuclear (with existing physical security standards of NRC applicable), hydroelectric, and coal (with neither NRC nor FERC physical security standards). Large coal-fired generating facilities should be protected against attack to prevent cascading outages and aid in system restoration.

None of the above comments on cost-effective measures were addressed in FERC Order No. 802.

[9] See Appendix 2, a Backgrounder prepared by the Nuclear Regulatory Commission in July 2014, on the evolution of Force-on-Force exercises sponsored by the Nuclear Regulatory Commission at nuclear power plant licensees, with NRC inspectors as observers. See also Appendix 3 to this Request for Rehearing, a commentary on Force-on-Force exercises prepared by Edwin Lyman of the Union of Concerned Scientists (UCS) dated March 21, 2014, , The UCS "insight" piece is reproduced with permission of UCS.

Request for Rehearing

Resilient Societies asserts that it is arbitrary and capricious for the Commission to disregard consideration of the above-specified issues. Moreover, it defies logic for the Commission to disregard the need for physical security standards for "High Impact" facilities not operated by transmission entities, while including a substantially larger group of "Medium Impact" facilities within the scope of Order No. 802.

For each of the issues presented and for the reasons provided, Resilient Societies respectfully requests that FERC schedule a rehearing to address the legal and technical merits of our Comments of September 8 and September 22, 2014.

To the extent that the evidentiary record in Docket RM14-15-000 did not specify and identify additional "High Impact" facilities and other "Medium Impact" facilities for which physical security standards would be just and reasonable, this was in part because Resilient Societies and other commentators sought to avert adversarial "targeting" of critical facilities within the Bulk Power System. Accordingly, Resilient Societies identifies and illustrates categories of "critical facilities" in need of physical security standards in an unredacted document filed under the privileged docket system but without admission that this publicly sourced information is subject to Critical Energy Infrastructure Information (CEII) restrictions.

Requests for Remand

Resilient Societies requests that FERC remand to NERC modifications of Reliability Standard CIP-014-1 to include:

1. Inclusion of Generator Operators with "High Impact" or "Medium Impact" facilities;
2. Inclusion of "High Impact" control centers and backup control centers of all Reliability Coordinators, with a period of consideration substantially shorter than the two years proposed by the Commission;

3. Inclusion of other specific facilities within the Bulk Power System that could cause cascading outage if attacked, with a period of consideration substantially shorter than the two years proposed by the Commission; and
4. The submission of a NERC program for the development and implementation of "Force-on-Force" security exercises that include FERC staff observers, modeled on the Force-on-Force exercise program of the Nuclear Regulatory Commission, so that critical facilities' programs for physical security are timely-evaluated and so "best practices" can be incorporated into physical security programs for the Bulk Power System.

Conclusion

Without rehearing, consideration of comments, and remand, FERC Order No. 802 will leave key facilities within the Bulk Power System vulnerable to physical attacks and combined physical and cyber-attacks. The Commission has an opportunity and the nation has a need for the Commission to revise its Order No. 802 and to commit NERC and its member utilities to adequate protection of the Bulk Power System.

When the FERC Commissioners consider this Request for Hearing, we respectfully ask that they respond to the specific points we raised in our docket Comments of September 8th and 22nd, laying out reasoning why our points are valid or not. Stating generally that "we are not persuaded" or ignoring a raised point is inconsistent with the requirements of case law under the Administrative Procedures Act. Were an attack on the Bulk Power System to result in a catastrophic outage, the American public would appropriately expect that the decisions of the FERC Commissioners had been fully documented and consistent with Section 215 of the Federal Power Act and other federal law.

Respectfully submitted by:

Thomas S. Popik, Chairman,

William R. Harris, Secretary,

For the
Foundation for Resilient Societies
52 Technology Way
Nashua, NH 03060-3245
www.resilientsocieties.org

APPENDIX 1

An unredacted version of Appendix 1 is filed under the privileged docket system for Critical Energy Infrastructure Information (CEII) for prudence but without admission that CEII provisions apply to publicly sourced information presented apart from within the context of this docket filing.

APPENDIX 2

United States Nuclear Regulatory Commission
Backgrounder on Force-on-Force Security Inspections

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

BACKGROUNDER
Office of Public Affairs
301.415.8200
www.nrc.gov ▪ opa.resource@nrc.gov

Force-on-Force Security Inspections

Security is a priority for the NRC - it is one of our strategic goals. Force-on-Force (FOF) inspections are an essential part of NRC's oversight of nuclear power plant security programs. After Sept. 11, the NRC upgraded security forces at nuclear facilities around the country. To test the security forces, the NRC implemented a more robust FOF inspection program.

The Nuclear Regulatory Commission has carried out FOF inspections regularly at commercial operating nuclear power plants since 1991 as part of its comprehensive security program. These inspections are an important way to evaluate and improve the effectiveness of plant security programs under NRC regulations (10 CFR Part 73) to prevent radiological sabotage.

FOF inspections assess a nuclear plant's physical protection measures to defend against the "design basis threat," or DBT. The DBT describes an adversary that plant owners must protect against with physical protection systems and response strategies. The NRC periodically reassesses the DBT and makes revisions as necessary.

A New, Stronger Force-on-Force Program

Before Sept. 11, 2001, NRC conducted FOF inspections about once every eight years at all U.S. nuclear plant sites, in addition to regular baseline security inspections. Following the Sept. 11 attacks, the NRC strengthened its FOF program, requiring plants to defend against a tougher DBT that reflected the new threat environment.

The NRC's redesigned FOF program was fully implemented by late 2004. Now, the NRC evaluates each plant site once every three years. All licensees conduct tactical security exercises in the intervening years. (The details of the FOF inspections are Safeguards Information, which is protected from public disclosure under the Atomic Energy Act.)

The program uses the supplemented DBT and greatly increases the level of realism, while ensuring the safety of plant employees and the public. NRC gives plant operators advance notice of FOF inspections for safety and logistical purposes and to provide for coordination of two sets of security officers — one for maintaining actual security, another for participating in the inspection. A key goal is to balance personnel safety, while maintaining actual plant security during exercises that are as realistic as possible.

Inspectors preparing FOF exercises use information from table-top drills, previous inspection reports and security plan reviews to design a number of commando-style attacks to probe potential weaknesses in the plant's defenses. The site's defenders aim to keep the attackers from destroying or damaging key equipment. Any potentially significant weaknesses in the protective strategy identified during FOF inspections are promptly addressed.

FOF inspection teams include active duty military advisors from the U.S. Special Operations Command. They help evaluate site security forces and systems, and provide an independent evaluation of the adversary force's performance.

NRC's force-on-force security inspections realistically test security forces' capability and security programs at nuclear power plants.

- *The NRC requires nuclear power plant operators to defend the plant against attackers seeking to damage the reactor core or spent fuel and cause a radiation release.*
- *During each FOF inspection, a number of commando-style attack exercises are carried out against a plant's security forces to test the plant operator's protective strategy.*
- *Any significant problems are promptly addressed.*
- *Each nuclear power plant site has at least one FOF inspection every three years.*
- *The NRC and plant operator ensure the safety of plant employees and the security of the plant during FOF exercises.*

Composite Adversary Force

A credible, well-trained, and consistent mock adversary force is vital to the FOF program. Prior to Sept. 11, power plant operators used adversary teams that often included security officers from their own sites, other licensees, and state police tactical team members. Using these diverse sources caused inconsistencies in the capabilities of the adversary team.

The revised FOF program uses a Composite Adversary Force (CAF) specifically trained to NRC standards. The CAF is a significant improvement over the previous mock "attack" forces.

NRC standards for the CAF cover the skills and physical fitness qualifications of team members; team tactics, communications and planning; firearms knowledge and proficiency; and exercise simulation equipment.

The CAF is managed by G4S, a company that provides security for a number of U.S. nuclear power plants and is well-versed in security operations. To avoid any conflict of interest, the NRC requires a clear separation of functions between the CAF and plant security forces. The NRC also maintains control over the design and implementation of the FOF inspections.

NRC's Overall Security Program

FOF inspections are an essential part of NRC's oversight of plant owners' security programs and their compliance with NRC security requirements. The agency continues to evaluate and strengthen its overall security program in response to changes in the threat environment, technological advancements and lessons learned. As a result, substantial improvements to nuclear plant security have been made to protect against terrorism and radiological sabotage. These include well-trained security forces, robust physical barriers, intrusion detection systems, surveillance systems and plant access controls.

Together, these efforts help make nuclear power plants among the best protected private sector facilities in the nation.

Additional information is available on NRC's website at www.nrc.gov/security.html. Other security backgrounders include:

- Dirty Bombs
- Nuclear Security Enhancements Since 9/11
- Safety and Security Improvements at Nuclear Plants

July 2014

APPENDIX 3

COMMENTARY BY ED LYMAN, UNION OF CONCERNED SCIENTISTS
ON NRC REQUIRED FORCE-ON-FORCE EXERCISES AT NRC LICENSED NUCLEAR POWER PLANTS

All Things Nuclear *Insights on Science and Security*

The NRC's Security Inspections at Nuclear Power Plants are Again under Attack

Ed Lyman, senior scientist

March 21, 2014

As President Obama is preparing to attend the third Nuclear Security Summit in The Hague next week, the United States is playing the "do as I say, not as I do" game concerning protection of commercial nuclear facilities against terrorist attacks.

The Nuclear Regulatory Commission (NRC), following the nuclear industry's lead, is carrying out major changes that could fatally undermine the effectiveness of its "force-on-force" inspection regimen, perhaps the world's most stringent program for conducting security oversight of commercial nuclear facilities. As the United States heads to the summit, it should lead by example and bolster the security of its nuclear facilities at home.

Instead, it is sending the wrong message by weakening its security requirements: reducing the number of tests that are conducted at each site and proposing to give more credit for tests that the plant owners conduct and grade themselves.

A similar effort at the Department of Energy (DOE) to decentralize security oversight under former Secretary Steven Chu contributed to a major security breach: the successful intrusion by three anti-war protesters into the Y-12 plant in Tennessee, the nation's main storehouse of bomb-usable highly enriched uranium. DOE is now trying to undo that mistake.

Why are Tests Important?

(Source: NRC)

Why is testing security performance with force-on-force (FOF) exercises essential? Because experience has shown that paperwork reviews of security plans cannot fully assess the actual, on-the-ground efficacy of security forces. The NRC requires facilities that are high-value terrorist targets be protected with "high assurance" against a "design basis threat" (DBT). The DBT lays out the NRC's assumptions about the general characteristics (weaponry, tactics, skills) of potential adversaries. For example, it requires nuclear power plants to be protected against an external attacking force (with the help of an insider) that seeks to damage safety systems and cause a Fukushima-type meltdown. U.S. experience at both military and civil facilities has shown that simply complying with regulations and standards is not sufficient to prove that security plans will work in practice. Since the 1990s, the NRC has been conducting force-on-force testing as part of its security inspections at nuclear power plants. According to a brochure issued by the NRC in October 2013 titled "Protecting Our Nation," FOF inspections are "an essential part of the oversight of the security of these facilities."
FOF inspections routinely uncover security vulnerabilities that require prompt correction. In the years preceding the 9/11 attacks, U.S. nuclear plants failed roughly 50 percent of their exercises, meaning that the mock attackers were able to simulate damaging enough equipment to result in a meltdown. After 9/11, the NRC required plant owners to make security upgrades and strengthened its inspection of those upgrades, in part to comply with a 2005 congressional mandate to conduct FOF tests every three years. After the NRC revamped the program, nuclear plants have been failing at a rate of about 5 percent on average, with no significant downward trend in the failure rate yet apparent.

Considering the horrific consequences of a real security failure, this rate is still too high and indicates there is room for improvement. Now is not the time for the NRC to take the pressure off the industry to protect its nuclear plants.

The Nuclear Industry Hates FOF Tests

One thing that has become obvious from monitoring the force-on-force inspection program for years is the industry despises it. This is understandable—no one likes to take tests. And just like schoolchildren who complain that a test was unfair when they don't do well, the industry has

persistently raised questions about the test protocols to try to diminish the significance of poor performance.

From my discussions with NRC inspectors, it is apparent that preserving an element of surprise is one of the most important factors to ensure that FOF tests are able to accurately measure nuclear plants' everyday security readiness. Of course, the exercises can never fully simulate a surprise attack: Nuclear plants must prepare for weeks before mock attacks so that they can be carried out safely. But there are aspects of a surprise FOF test that can help ensure the exercises are challenging. One important factor is the independence of the mock attack force. The attack force should be free to choose any attack scenario as long as it is consistent with the capabilities of the design basis threat, even if it employs those capabilities in new ways

The NRC also has to make sure that the attack force cannot collude with defending forces to "fix" the tests. It will be difficult for the agency to maintain the necessary separation if the mock attackers are made up of plant security force members, since there is a potential for conflict of interest.

In the first iteration of its FOF inspections in the 1990s, the NRC used actual members of the U.S. Army Special Forces (whom it referred to euphemistically as "subject matter experts") as an integral part of the team that planned and carried out the mock attacks. But apparently they were too good at their jobs. After industry complaints, and a brief cancellation of the program, the industry proposed that the NRC replace the FOF inspections with a self-assessment program, in which the licensees themselves would staff and run the FOF drills and the NRC would be relegated to the role of a passive observer. This raised concerns among some NRC staff, who feared that this could whittle down the exercises to mere dog-and-pony shows in which the licensees would stage well-rehearsed performances for the NRC inspectors' benefit.

Inadequate Tests, Even after 9/11…

The 9/11 attacks partly derailed this effort and prompted the NRC to strengthen the FOF inspections and increase their frequency from one every eight years to one every three years. However, the NRC has downgraded the subject matter experts' role in the current program, and the tests use an industry-run "composite adversary force" (CAF) instead. The NRC says that it avoids conflict of interest issues by requiring "a clear separation of functions between the CAF and plant security forces."

Nevertheless, questions remain about whether the post-9/11 inspection program is as rigorous and independent as the earlier program. In addition, numerous other artificialities compromise the tests' realism, including strict limitations on the role insiders could play in assisting in attack planning, and no requirement to consider simultaneous cyberattacks.

Unfortunately, the industry has never given up on the idea of substituting its own FOF drills for the NRC-run inspections, and now the NRC seems more open than ever to allowing this to happen. The Nuclear Energy Institute (NEI), the industry's primary trade association, formed an "Alternate

Approach to FOF Focus Group" in February 2013, which is promoting a very similar approach to the self-assessment program it proposed before the 9/11 attacks.

… and Maybe Worse to Come

In response to industry complaints, the NRC already has reduced the number of FOF exercises per inspection from three to two and is proposing to reduce it to only one by 2017. In exchange, the NRC will give more credit to licensee-run security drills and will observe one such drill in each inspection cycle. This is a slippery slope toward the industry's ultimate goal: to take control of the process and eliminate the potentially embarrassing FOF exercises altogether. Even worse, the NRC commissioners have directed the staff to review the entire FOF program with an apparent eye toward weakening it even further.

On top of that, NRC commissioners are apparently questioning the agency's policy that plant owners should immediately correct all security vulnerabilities detected during FOF inspections.

If the NRC continues on its current course, the potential for terrorists to trigger a Fukushima-like meltdown at a U.S. nuclear plant—already unacceptably large, in our view—will only increase.

More information on NRC and industry plans and UCS's response can be found here.

Posted in: Nuclear Power Safety, Nuclear Terrorism Tags: NRC, nuclear power, nuclear power safety, nuclear terrorism

About the author: Dr. Lyman received his PhD in physics from Cornell University in 1992. He was a postdoctoral research scientist at Princeton University's Center for Energy and Environmental Studies, and then served as Scientific Director and President of the Nuclear Control Institute. He joined UCS in 2003. He is an active member of the Institute of Nuclear Materials Management and has served on expert panels of the Nuclear Regulatory Commission. His research focuses on security issues associated with the management of nuclear materials and the operation of nuclear power plants, particularly with respect to reprocessing and civil plutonium. Areas of expertise: Nuclear terrorism, proliferation risks of nuclear power, nuclear weapons policy.