NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: Commission Ostendorff

SUBJECT: SECY-16-0073: OPTIONS AND RECOMMENDATIONS FOR THE FORCE-ON-FORCE INSPECTION PROGRAM IN RESPONSE TO SRM-SECY-14-0088

Approved XX Disapproved XX Abstain ____ Not Participating ____

COMMENTS: Below ____ Attached XX None ____

Entered in STARS
Yes X
No ____

/RA/
Signature

6/28/16
Date

Commissioner Ostendorff's Comments on SECY-16-0073:
"Options and Recommendations for the Force-On-Force Inspection Program in Response to SRM SECY 14-0088"

It is my intent in this vote to share with the staff and my fellow Commissioners my thoughts on security regulatory matters in a broad context rather than limit my comments to the specific matters discussed in SECY-16-0073.

As discussed in COMWCO-14-0001/COMGEA-14-0001, and subsequently in my vote on SECY-14-0088, the current force-on-force program has been in place for twelve years, and significant security enhancements have been implemented by licensees since the terrorist attacks of September 11, 2001. I have confidence through our licensing and oversight programs that commercial nuclear power facilities are protected by robust security measures.

A Commission-directed lessons-learned review of the force-on-force program was initiated in 2014 and resulted in enhancements and clarifications to the force-on-force program in several areas. These areas include the timing of compensatory measures and the realistic ability to exploit unattended openings. Other staff-initiated changes were implemented over the past two years including reducing the number of exercises during triennial force-on-force inspections from three to two, increasing notification time for force-on-force inspections to allow more effective resource planning, and enhancing the significance determination process for security. I applaud the staff's actions in these areas.

Recently, industry has suggested reducing the number of force-on-force exercises from two to one. I do not support this proposal. While this could result in some resource savings, it could also introduce challenges if the exercise is indeterminate due to controller issues or must be cancelled due to inclement weather or other unforeseen circumstances. The staff should evaluate a change to the force-on-force program wherein the staff would plan two exercises and establish criteria to permit the staff to cancel the second exercise if the licensee demonstrates an effective protective strategy in the first exercise and has no significant performance deficiencies in the security cornerstone. On a related matter, it is important to note that force-on-force exercises are designed to be very challenging and that a "failed" force-on-force exercise does not necessarily indicate that a licensee's protective strategy is ineffective or noncompliant. Any performance deficiencies identified during the force-on-force inspection or other security inspections must be appropriately evaluated through the significance determination process. The need for changes to a licensee's protective strategy in response to inspection findings must be evaluated carefully in the context of the licensing basis and backfit considerations.

I am also opposed to industry's suggestion that the NRC observe licensee-conducted force-on-force exercises in lieu of NRC-conducted force-on-force exercises. This should not be viewed as criticism of licensee efforts. Rather, NRC-conducted force-on-force exercises have an important role in the public confidence in physical security programs and are mandated by

legislation. Furthermore, NRC-conducted force-on-force exercises establish a consistent and structured framework to fulfill the agency's regulatory responsibilities.

As a Commissioner, my votes have been grounded in the NRC's longstanding regulatory framework of adequate protection and the application of the backfit rule. I have also been guided by the principles of good regulation. Consistent with our principles of good regulation, regulatory activities should be consistent with the degree of risk reduction they achieve, and once established should be perceived as reliable and not unjustifiably in a state of transition. In that context, in my deliberations on safety matters, I ask the questions: "What problem are we trying to fix?" and "How safe is safe enough?" As I read SECY-16-0073, and as I listened to discussions during a recent Commission meeting on related topics, I was struck that we must exercise the same degree of discipline in regulatory decisions on security matters as we do on safety matters and ask similar questions: "What problem are we trying to fix?" and "How secure is secure enough?"

I would also like to provide some context for the Commission's recent direction to the staff in SRM-M160623 to provide proposed revisions to Regulatory Guides 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements" and 5.77, "Insider Mitigation Program," to the Commission for review and approval. The Commission is responsible for establishing the Design Basis Threat (DBT) and approving any proposed changes to the DBT based on the threat environment. To fulfill this obligation, the Commission has access to current intelligence information through frequent briefings and interactions with federal law enforcement and intelligence agencies. The Commission also has awareness of the broader context of security requirements within the NRC's regulatory framework, and therefore has the ability to view safety and security protections as one integrated regime that assures adequate protection of public health and safety. For these reasons, proposed revisions to the DBT and associated regulatory guides should be subject to Commission-level review and approval.

Further reinforcing this direction, I will note that there is scant explanation in our regulatory history of the basis for the standard of "high assurance" used in Part 73 to ensure adequate protection of public health and safety. It is the Commission's responsibility to provide direction to the staff, and this vote paper offers an appropriate means to clarify what "high assurance" is. Through discussions with senior NRC staff and review of the Part 73 statements of consideration, it is my understanding that when it introduced the term "high assurance," the Commission did not intend to establish a separate standard for security regulations. Instead, as explained in 1979, when the Commission updated Part 73 and revised its "high assurance" objective in the performance of security systems, the Commission explained that "'reasonable assurance,' commonly used in safety evaluations, is applied to a broad category of safety concerns. . . . [T]he degree of assurance necessary to provide 'reasonable assurance' varies with the gravity of the safety concern." 44 Fed. Reg. 68,184, 68,185 (Nov. 28, 1979). Thus, the regulatory standard for security is the same as the regulatory standard for safety—reasonable

assurance of adequate protection of public health and safety—and the Commission sets the standard.

I will now turn to the use of quantitative analysis to evaluate regulatory changes on security matters. I recognize that tools such as probabilistic risk assessment are more easily applied to regulatory decisions in the safety arena. However, the same regulatory framework and backfit provisions apply to both safety and security requirements. Any proposed changes to security requirements and guidance should be supported by thorough regulatory analysis and quantitative analysis to the extent practical. Vulnerability assessment tools may be of use to evaluate proposed regulatory requirements and to assess licensees' protective strategies, for example the size of the licensees' protective force.

Finally, with regard to the specific recommendations in SECY-16-0073, I approve the staff's proposal in Option 1 to terminate the Tactics, Techniques, and Procedures Working Group. All follow-on activities from the Working Group and the direction received from the Commission should be conducted by the program offices. Regarding Option 2, the staff has not made it clear what problem they are trying to fix, what the expected outcomes are, and what resources would be required. In the current budgetary environment we cannot spend resources on new projects without a clear understanding of the objective. Therefore, I disapprove Option 2. Instead of Option 2, the staff should evaluate the following issues and provide a notation vote paper discussing any proposed actions:

1. Evaluate how vulnerability assessments could be used to evaluate the effectiveness of licensee protective strategies, and whether credit could be given for operator actions or for the use of additional equipment such as "flex equipment," which was installed to enhance safety but can also provide a security benefit.
2. Evaluate whether the NRC should provide any credit for local state or federal law enforcement response to establish coping time for security events. For example, if a licensee engages with state and local law enforcement to conduct site familiarization tours and site security exercises, could the staff give credit for integrated response capability in establishing the required coping time for a security event?
3. Evaluate the NRC's historical application of the backfit rule to security decision-making and whether additional guidance is needed in this area regarding the ability to quantify the benefit of security enhancements.