ANTHONY R. PIETRANGELO
Senior Vice President and Chief Nuclear Officer
Nuclear Generation

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8081
arp@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

February 25, 2016

The Honorable Stephen G. Burns
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Request for Closed Commission Meeting on Security

Project Number: 689

Dear Chairman Burns:

We would like to request a closed meeting with the Commission to discuss the state of security at the nation's nuclear power facilities. This September will mark the 15-year anniversary of the September 11, 2001 terrorist attacks. Since that time, the commercial nuclear power industry has invested in excess of 2 billion dollars to enhance its security posture and ability to protect against increased physical and cyber threats to its facilities. You may recall that in the years following the attacks, the Commission met with industry in numerous closed meetings to discuss a range of security issues. These issues included potential changes to the design basis threat ("DBT"), and policy issues associated with force-on-force exercises. We believe the last closed meeting between industry and the Commission was almost seven years ago.

The work of the Commission and industry in response to the September 11 attacks has substantially enhanced the physical and cyber security of the commercial nuclear power fleet, making these facilities the nation's hardest industrial targets. That said, we are concerned that the agency continues to seek additional security measures absent any apparent change in the overall threat environment, or meaningful backfit or cost benefit analyses. Most recently, policy issues have arisen in several areas, including the agency's force-on-force, cyber security, and insider mitigation programs.

Now in its fourth cycle, force-on-force exercises are central to the NRC security inspection program. They have successfully demonstrated, with high assurance, that a licensee's protective strategy is adequate to protect against threats that are consistent with the DBT. We acknowledge that over the last few years, the NRC has made adjustments to these exercises to ensure the inspection objectives are achieved in a more

efficient and effective manner. However, we continue to observe the imposition of tactics and techniques that we believe are unrealistic and exceed the DBT. In addition, the staff is currently considering revisions to the adversary characteristics described in Regulatory Guide 5.69 that would, in our view, modify the DBT. This process bypasses the important role of the Commission in exercising its oversight and would seem to allow the staff to revise settled regulation.

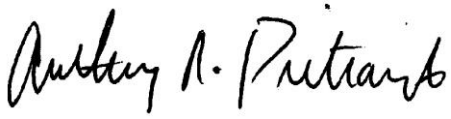
In the area of cyber security, we are concerned that a recent change in staff position would potentially expand the scope of the cyber security program to cover the Personal Access Data System (PADS) and other access authorization systems. The PADS system is, in our view, outside the scope of the cyber security rule. And, notably, the industry has taken appropriate measures to mitigate cyberattacks that would preclude individuals from gaining unauthorized access to the protected area by cyber means.

Finally, we have concerns regarding changes in the staff's position regarding the mitigation of threats posed by "insiders." Mitigation of such threats is part of the DBT and was the subject of numerous discussions with the Commission and the NRC staff leading up to promulgation of the security regulations in 10 CFR Part 73. As a result of these discussions, the NRC and industry agreed on the elements of an insider mitigation program[1]. The industry has also implemented behavioral observation programs and actions to evaluate the initial and ongoing trustworthiness and reliability of individuals, irrespective of their technical competencies. The recently issued Regulatory Guide 5.77 includes guidance that treats insider mitigation for the cyber threat differently from insider mitigation for the DBT generally. The industry has historically treated the cyber threat as part of the DBT and the mitigation programs previously accepted by the agency apply to all facets of the DBT, including cyber threats. Therefore, we believe it is inappropriate and unnecessary for staff to impose, absent a basis for change, new expectations for the mitigation of cyber threats through the insider mitigation program.

The concerns detailed above share a common cause of being, to our knowledge, unanchored from a current threat assessment. Without a firm basis, these changes to guidance and interpretations have undermined the stability of security regulation. Continued dialogue between industry leadership and the Commission is essential to ensure that the agency's security programs are maintained in a manner that both provides for the common defense and security and adheres to the Commission's Principles of Good Regulation.

We appreciate your consideration of this request.

Sincerely,



Anthony R. Pietrangelo

[1] Letter from Mr. Roy Zimmerman (NRC) to Mr. Steven Floyd (NEI) April 5, 2004.

c: The Honorable Kristine Svinicki
The Honorable William Ostendoff
The Honorable Jeffery Baran
Victor McCree, EDO
Michael Johnson, DEDO
Brian Holian, Director, NSIR

CHAIRMAN Resource

From:	PIETRANGELO, Tony <arp@nei.org>
Sent:	Thursday, February 25, 2016 8:29 AM
To:	CHAIRMAN Resource
Cc:	Svinicki, Kristine; CMROSTENDORFF Resource; CMRBARAN Resource; McCree, Victor; Johnson, Michael; Holian, Brian
Subject:	[External_Sender] Request for Closed Commission Meeting on Security
Attachments:	02-25-16_NRC_Request for Closed Commission Meeting on Security.pdf

February 25, 2016

The Honorable Stephen G. Burns
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Request for Closed Commission Meeting on Security

Project Number: 689

Dear Chairman Burns:

We would like to request a closed meeting with the Commission to discuss the state of security at the nation's nuclear power facilities. This September will mark the 15-year anniversary of the September 11, 2001 terrorist attacks. Since that time, the commercial nuclear power industry has invested in excess of 2 billion dollars to enhance its security posture and ability to protect against increased physical and cyber threats to its facilities. You may recall that in the years following the attacks, the Commission met with industry in numerous closed meetings to discuss a range of security issues. These issues included potential changes to the design basis threat ("DBT"), and policy issues associated with force-on-force exercises. We believe the last closed meeting between industry and the Commission was almost seven years ago.

The work of the Commission and industry in response to the September 11 attacks has substantially enhanced the physical and cyber security of the commercial nuclear power fleet, making these facilities the nation's hardest industrial targets. That said, we are concerned that the agency continues to seek additional security measures absent any apparent change in the overall threat environment, or meaningful backfit or cost benefit analyses. Most recently, policy issues have arisen in several areas, including the agency's force-on-force, cyber security, and insider mitigation programs.

Now in its fourth cycle, force-on-force exercises are central to the NRC security inspection program. They have successfully demonstrated, with high assurance, that a licensee's protective strategy is adequate to protect against threats that are consistent with the DBT. We acknowledge that over the last few years, the NRC has made adjustments to these exercises to ensure the inspection objectives are achieved in a more efficient and effective manner. However, we continue to observe the imposition of tactics and techniques that we believe are unrealistic and exceed the DBT. In addition, the staff is currently considering revisions to the adversary characteristics

described in Regulatory Guide 5.69 that would, in our view, modify the DBT. This process bypasses the important role of the Commission in exercising its oversight and would seem to allow the staff to revise settled regulation.

In the area of cyber security, we are concerned that a recent change in staff position would potentially expand the scope of the cyber security program to cover the Personal Access Data System (PADS) and other access authorization systems. The PADS system is, in our view, outside the scope of the cyber security rule. And, notably, the industry has taken appropriate measures to mitigate cyberattacks that would preclude individuals from gaining unauthorized access to the protected area by cyber means.

Finally, we have concerns regarding changes in the staff's position regarding the mitigation of threats posed by "insiders." Mitigation of such threats is part of the DBT and was the subject of numerous discussions with the Commission and the NRC staff leading up to promulgation of the security regulations in 10 CFR Part 73. As a result of these discussions, the NRC and industry agreed on the elements of an insider mitigation program[1]. The industry has also implemented behavioral observation programs and actions to evaluate the initial and ongoing trustworthiness and reliability of individuals, irrespective of their technical competencies. The recently issued Regulatory Guide 5.77 includes guidance that treats insider mitigation for the cyber threat differently from insider mitigation for the DBT generally. The industry has historically treated the cyber threat as part of the DBT and the mitigation programs previously accepted by the agency apply to all facets of the DBT, including cyber threats. Therefore, we believe it is inappropriate and unnecessary for staff to impose, absent a basis for change, new expectations for the mitigation of cyber threats through the insider mitigation program.

The concerns detailed above share a common cause of being, to our knowledge, unanchored from a current threat assessment. Without a firm basis, these changes to guidance and interpretations have undermined the stability of security regulation. Continued dialogue between industry leadership and the Commission is essential to ensure that the agency's security programs are maintained in a manner that both provides for the common defense and security and adheres to the Commission's Principles of Good Regulation.

We appreciate your consideration of this request.

Sincerely,

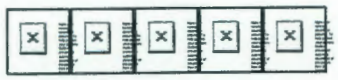
Anthony R. Pietrangelo
Senior Vice President and Chief Nuclear Officer

Nuclear Energy Institute
1201 F Street NW, Suite 1100
Washington, DC 20004
www.nei.org

P: 202.739.8081
M: 202.439.2511
E: arp@nei.org

TAKE THE NEI FUTURE OF ENERGY QUIZ, www.NEI.org/futureofenergy

FOLLOW US ON



---

[1] Letter from Mr. Roy Zimmerman (NRC) to Mr. Steven Floyd (NEI) April 5, 2004.