UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

August 11, 2011

The Honorable Gregory B. Jaczko
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: RESPONSE TO THE JUNE 8, 2011, EDO LETTER REGARDING DRAFT FINAL REVISION 3 OF REGULATORY GUIDE (RG) 1.152, "CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS"

Dear Chairman Jaczko:

During the 585th meeting of the Advisory Committee on Reactor Safeguards (ACRS), July 13-15, 2011, we reviewed the Executive Director for Operations (EDO) response dated June 8, 2011, to the April 20, 2011, ACRS letter on draft final RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."

BACKGROUND

RG 1.152, Revision 3, separates the safety licensing design review of Digital Instrumentation and Control (DI&C) systems from the cyber security design review by specifically stating that there will not be any review of the hardware and software to meet the defensive architecture guidance in RG 5.71, "Cyber Security Programs for Nuclear Facilities," when the safety review is performed.

DISCUSSION

In our report of April 20, 2011, we recommended that, "Explicit statements that the licensing design reviews will not address cyber security design features for other than their effect on the safety system should be deleted. Licensees should understand that as part of the safety system review, all features of their designs will be reviewed for licensing purposes, including cyber security, to the extent possible."

In their response to our report, the staff argued that they cannot incorporate this recommendation because "…it is inconsistent with the existing regulatory framework. The staff will retain the language of RG 1.152, Revision 3 to ensure consistency with 10 CFR 73.54 which is a performance-based regulation. The 10 CFR 73.54 contains language that precludes detailed review of cyber security features during licensing."

We bring this issue to your attention to point out the importance of finding or creating a path forward that would ensure integrating the safety and security reviews. RG 5.71 describes defense-in-depth protective strategies and technical controls as primary measures to thwart malicious cyber attacks. It states that "The technical controls are safeguards or protective measures that are executed through hardware, firmware, operating systems, or application software. These controls are not accomplished through administrative procedures and human actions."

The ability of digital safety and non-safety systems to thwart malicious attacks depends on fundamental capabilities of the hardware and software architectures to implement the measures needed to meet the requirements of the cyber security plan. Both the safety and security reviews require the same detailed technical understanding of the computer system, albeit judging that system against different criteria. To delay an inspection against cyber-based threats until the design has fully evolved and is set in hardware, firmware, and software may result in defenses that are less efficient and less effective than could be achieved if known issues were addressed in an integrated manner early in the design stage.

The staff also argued that, due to the evolving nature of technology and the cyber threats, examination during the safety review "…could generate a false sense of confidence given the evolving nature of cyber-based threats." Delaying review of the DI&C architecture against cyber threats introduces the greater risk of false confidence in the design. We are not advocating a final determination regarding the adequacy of the design to mitigate unforeseen future security threats. Ensuring that the architectures are consistent with safety and cyber security requirements does not preclude changes at the device level as the design matures or as technology evolves.

Sincerely

/RA/

Said Abdel-Khalik
Chairman

References:

1. Letter to Dr. Said Abdel-Khalik, ACRS, Response to Advisory Committee on Reactor Safeguards Recommendations on Draft Final Revision 3 of Regulatory Guide 1.152, "Criteria for Use of Computer in Safety Systems of Nuclear Power Plants," 06/08/2011 (ML111390059)

2. Letter to Mr. R.W. Borchardt, EDO, Draft Final Revision 3 of Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," 04/20/2011 (ML11112A140)

3. Draft Final RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Rev. 3, 01/21/2011 (ML110200231)

4. Regulatory Guide RG 5.71, "Cyber Security Programs for Nuclear Facilities," Rev 0, January 2009 (ML090760860)

References:

1. Letter to Dr. Said Abdel-Khalik, ACRS, Response to Advisory Committee on Reactor Safeguards Recommendations on Draft Final Revision 3 of Regulatory Guide 1.152, "Criteria for Use of Computer in Safety Systems of Nuclear Power Plants," 06/08/2011 (ML111390059)

2. Letter to Mr. R.W. Borchardt, EDO, Draft Final Revision 3 of Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," 04/20/2011 (ML11112A140)

3. Draft Final RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Rev. 3, 01/21/2011 (ML110200231)

4. Regulatory Guide RG 5.71, "Cyber Security Programs for Nuclear Facilities," Rev 0, January 2009 (ML090760860)

Accession No:ML11199A149 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	CSantos	EHackett	EMH for SAK
DATE	08/04 /11	08/04/11	08/09/11	08/10 /11	08/10/11

OFFICIAL RECORD COPY

Letter to the Honorable Gregory B Jaczko, Chairman, NRC, from Said Abdel-Khalik, Chairman, ACRS, dated August 11, 2011

SUBJECT: RESPONSE TO THE JUNE 8, 2011, EDO LETTER REGARDING DRAFT FINAL REVISION 3 OF REGULATORY GUIDE (RG) 1.152, "CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS"

Distribution:
ACRS Staff
ACRS Members
B. Champ
A. Bates
L. Mike
A. Lewis
M. Orr
C. Jaegers
K. Clayton
RidsSECYMailCenter
RidsEDOMailCenter
RidsNMSSOD
RidsNSIROD
RidsFSMEOD
RidsRESOD
RidsOIGMailCenter
RidsOGCMailCenter
RidsOCAAMailCenter
RidsOCAMailCenter
RidsNRROD
RidsNROOD
RidsOPAMail
RidsRGN1MailCenter
RidsRGN2MailCenter
RidsRGN3MailCenter
RidsRGN4MailCenter