

**Official Transcript of Proceedings**  
**NUCLEAR REGULATORY COMMISSION**

Title: Public Workshop to Discuss I&C Cyber  
Security-by-design and Associated  
Potential Regulatory Impacts

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, April 9, 2015

Work Order No.: NRC-1501

Pages 1-97

**NEAL R. GROSS AND CO., INC.**  
**Court Reporters and Transcribers**  
**1323 Rhode Island Avenue, N.W.**  
**Washington, D.C. 20005**  
**(202) 234-4433**

## U.S. NUCLEAR REGULATORY COMMISSION

+ + + + +

## OFFICE OF NEW REACTORS

+ + + + +

## PUBLIC WORKSHOP TO DISCUSS I&amp;C

## CYBER SECURITY-BY-DESIGN AND

## ASSOCIATED POTENTIAL REGULATORY IMPACTS

+ + + + +

THURSDAY

APRIL 9, 2015

+ + + + +

The Public Workshop met in Rooms 01C03 and 01C05, NRC Headquarters, Three White Flint North, 11601 Landsdown Street, Rockville, Maryland, at 8:30 a.m.

NRC STAFF PRESENT

CATHERINE ALLEN, NSIR/CSD

SUSHIL BIRLA, RES/DE

BERNARD DITTMAN, RES/DE/ICEEB

RUSS FELTS, NSIR/CSD

TERRY JACKSON, NRO/DE/ICE1

MICHAEL JONES, NRO/DARR/ARPB

IAN JUNG, NRO/DE/ICE2

RUI LI, NSIR/CSD

ERICK MARTINEZ, RES/DE/ICEEB

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

JONAH PEZESHKI, NSIR/CSD

PAUL REBSTOCK, RES/DE/ICEEB

DAVID RAHN, NRR/DE/EICB

JOHN RYCINA, NSIR/CSD

RICHARD STATTEL, NRR/DE/EICB

JOHN TAPPERT, NRO/DE

BARRY WESTREICH, NSIR/CSD

DEANNA ZHANG, NRO/DE/ICE1

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

## TABLE OF CONTENTS

Welcome and Meeting Logistics .....	4
Introductions of Participants .....	6
NRC Staff Topical Presentation .....	8
Facilitated Open Discussion .....	23
Opportunity for Public Comment .....	91
Closing Remarks/Adjourn .....	96

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

P-R-O-C-E-E-D-I-N-G-S

(8:31 a.m.)

MR. JONES: Good morning, everyone, and thanks for coming to the meeting on I&C Cyber Security-By-Design Discussion.

This is a Category 2 Public Meeting. That means that there will be an opportunity for the public to make comments and to ask questions of the NRC Staff at specific times on the agenda.

Let's see. We've got some logistics. In case there's a fire or an emergency, we're going to exit this room. We're going to go out through the guard station. We'll muster outside. We'll make sure that everybody on the sign-up list is with us.

And there are bathrooms around the corner. Over by the cafeteria on this floor. No escorts required on this floor.

The meeting is going to be transcribed. So, we're going to ask that everyone that speaks please use the microphone. I'll be happy to bring one to you at any time. Let's talk one at a time and please put your phone on vibrate or turn them off.

For folks on the line, please make sure

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 that your phones are muted. You can do that by  
2 hitting star-6 and I'll cue you in when there's  
3 times for the public and for industry on the phone  
4 to jump into the discussion.

5 Our agenda is a bit flexible today. It  
6 depends on the amount of discussion. We didn't  
7 have any industry submittals or presentations.  
8 So, after our presentation, we'll go right into NRC  
9 and industry discussion Q&A.

10 We've got a couple of speakers to lead.  
11 First, I'd like to introduce Russ Felts and he's  
12 the Deputy Director of the Cyber Security  
13 Directorate from the Nuclear Security and Incident  
14 Response Office at the NRC.

15 Russ.

16 MR. FELTS: Yes, I really just wanted  
17 to offer a few comments to sort of frame the  
18 discussion.

19 I suspect that a lot of folks who are  
20 participating in this meeting might be concerned  
21 that what we're contemplating here is to require  
22 design cert applicants to demonstrate how they will  
23 meet requirements of 73.54 and I wanted to clarify  
24 for anybody that has that misconception that what  
25 we're talking about here is not broad consideration

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 of how cyber security is met at the design stage.

2 But more properly a very narrow look at  
3 certain aspects of cyber security during the design  
4 stage and really looking at finding ways to enable  
5 a designer to show that the design that they have  
6 proposed is not going to be so challenging to  
7 actually implement the cyber security program that  
8 the COL applicant would have some outrageously  
9 difficult program to have to implement in order to  
10 meet requirements of 73.54.

11 So, we're going to get into a lot more  
12 discussion of that. But I just wanted to lead off  
13 the discussion so folks aren't percolating over  
14 that, you know, misconception throughout the  
15 meeting.

16 MR. JONES: Next, we have Deanna Zhang  
17 who's going to give some introductions and she'll  
18 be leading us through the staff presentation and  
19 I guess ordinarily we just go around the room and  
20 get everybody's name, but why don't we wait and as  
21 speakers come, you give your name and your  
22 affiliation. We'll get it that way.

23 Okay. We'll go around. So, just pass  
24 a mic down and --

25 MR. LI: Rui Li with NSIR/CSD.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 MR. MARTINEZ: Erick Martinez, NRC  
2 Research.

3 MR. JACKSON: Terry Jackson, Office of  
4 New Reactors.

5 MR. JARRETT: Ron Jarrett, TVA,  
6 Digital Program Manager.

7 MR. HERB: Ray Herb, Southern Nuclear,  
8 I&C Design.

9 MR. BAILEY: Mike Bailey, Duke Energy,  
10 Engineering Director for Digital Engineering  
11 Support.

12 MR. WESTREICH: Barry Westreich,  
13 Director, Cyber Security Directorate, NRC.

14 MR. FELTS: Russ Felts, Deputy  
15 Director, Cyber Security Directorate.

16 MR. YEATES: Brad Yeates, Southern  
17 Company, Cyber Security Program.

18 MR. CONNELLY: John Connelly, Exelon,  
19 Cyber Security Program Manager.

20 MR. GROSS: Bill Gross, NEI.

21 MR. BIRLA: Sushil Birla, NRC  
22 Research.

23 MR. RYCINA: John Rycyna, NSIR/CSD.

24 MS. ALLEN: Cathy Allen, NSIR/CSD.

25 MR. DITTMAN: Bernie Dittman, NRC

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 Research.

2 MR. CLARKSON: Greg Clarkson, NuScale  
3 Power, Reactor Protection System Design.

4 MR. GIBSON: Matt Gibson, Electric  
5 Power Research Institute.

6 MS. BERGMAN: Jana Bergman, Sciencetech.

7 MR. JUNG: Ian Jung, NRC, Office of New  
8 Reactors.

9 MR. TAPPERT: John Tappert, NRC,  
10 Office of New Reactors.

11 MR. REBSTOCK: Paul Rebstock, office  
12 of Research.

13 MR. RAHN: David Rahn, Office of NRR.

14 MR. PEZESHKI: Jonah Pezeshki,  
15 NSIR/CSD. Also, the leader of the Cyber  
16 Assessment Team.

17 MS. ZHANG: Deanna Zhang, Office of New  
18 Reactors.

19 MR. STATTEL: Rich Stattel, NRR.

20 MS. ZHANG: Let me move this a little  
21 closer than that. Can you guys hear me? Good.  
22 Okay.

23 So, good morning. I would like to  
24 welcome everyone here to our Cyber Security Design  
25 Requirements Workshop and I would like to thank you

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 guys for traveling here. I know some of you guys  
2 had to travel pretty far and also look forward to  
3 discussing some the potential options we're  
4 thinking about for incorporating cyber security  
5 design requirements into the NRC's regulations.

6 Next slide. So, I know that Russ kind  
7 of laid out the scope a little bit, but I wanted  
8 to go into it a little bit further.

9 We're planning on discussing options  
10 for including cyber security design requirements  
11 into power reactors into the NRC regulations and  
12 we just want to emphasize we're not planning to  
13 discuss any other cyber security initiatives such  
14 as the NEI petition for cyber security rulemaking.  
15 We understand that there are other venues to  
16 address those activities.

17 Next slide. So, during today's  
18 presentation, we'll be providing an overview of  
19 potential options. We're including cyber  
20 security design requirements into the NRC's  
21 regulations. These options will only apply to  
22 power reactors including both new and operating  
23 reactors.

24 And keep in mind, these are only, you  
25 know, our own initial thoughts. So, we would like

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 to solicit your feedback regarding these potential  
2 options and maybe, you know, if there are new  
3 options that we have not considered yet, we would  
4 like to listen to them.

5 And also, we're not looking to add new  
6 technical requirements, but maybe changing some of  
7 our licensing process to see if we can perform some  
8 of the reviews of cyber security technical controls  
9 during licensing. But, in order to do so, it might  
10 entail some rulemaking. So, this is much more of  
11 a process change than, you know, any new technical  
12 requirements.

13 Next slide. So, before we present the  
14 different options we're considering, let me just  
15 go off some of the background with respect to, you  
16 know, our current regulatory frameworks and the  
17 guidance that's available to kind of set the stage.

18 So, the following the events of  
19 September 11th, the NRC underwent a comprehensive  
20 review of the security requirements and potential  
21 vulnerabilities at our regulated nuclear  
22 facilities. The NRC issued security orders more  
23 to impose requirements to enhance security and this  
24 included consideration of cyber security. This is  
25 a bubble was already required. What was required

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 in the regulation at that time.

2 Subsequently, the NRC published NUREG  
3 68.47 which provided guidance in methodology for  
4 conducting cyber security self-assessment.

5 And following in 2005, the NRC endorsed  
6 NEI 04-04 which also provided guidance for  
7 developing and maintaining a cyber security  
8 program at licensed nuclear facilities and at that  
9 time, the licensees had committed to implement  
10 voluntarily NEI 04-04.

11 In 2009, the NRC issued 10 CFR 73.54.  
12 This is the regulation which required licensees to  
13 provide high assurance that digital computers and  
14 communicate systems and networks are adequately  
15 protected against a cyber attack.

16 And following in 2010, the NRC  
17 published Reg Guide 5.71 which provided an  
18 acceptable method for complying with the  
19 requirements of 10 CFR 73.54.

20 Next slide. In 2010, the NRC endorsed  
21 NEI 08-09 which was developed by NEI to assist  
22 licensees in complying with the requirements of 10  
23 CFR 73.54. So, licensees could either use 10 CFR  
24 -- oh, could use NEI 08-09 or 10 CFR or Reg Guide  
25 5.71.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           In 2011, the NRC issued Revision 3 to  
2 Reg Guide 1.152 and just to remind everyone, in  
3 Revision 2 of this Reg Guard, the NRC did include  
4 guidance to address cyber security because we  
5 didn't have any other means to address cyber  
6 security at that time.

7           However, since 10 CFR 73.54 was issued  
8 along with its complementing reg guide, we removed  
9 that, the cyber security portion, guidance within  
10 that regulatory guide.

11           We still kept apportioned direct access  
12 controls which is to establish a secure development  
13 operational environment for digital safety systems  
14 where measures should be included to direct any  
15 non-malicious vulnerabilities that's in the  
16 design. More to insure integrity, reliability and  
17 functionality of the digital safety system while  
18 it's in operation.

19           And lastly, in 2013, the NRC endorsed  
20 NEI 13-10 which was developed to provide guidance  
21 for implementing a consequence based approach to  
22 implementation of the cyber security controls for  
23 the length of these critical digital assets.

24           So, let's go a little bit more into the  
25 10 CFR 73.54. I just want to make sure we're on

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 the right slide.

2 So, 10 CFR 73.54, it provides a  
3 programmatic regulatory framework for the  
4 licensees and COLs to protect digital computer and  
5 communication systems and networks against cyber  
6 attacks. So, I want to emphasize it's  
7 programmatic based.

8 It requires licensees and COL  
9 applicants to submit a cyber security plan that is  
10 reviewed by the NRC. However, this regulation  
11 does not require licensees and COL applicants to  
12 submit any cyber security design information for  
13 NRC licensing review. It also does not require  
14 design certification applicants to submit design  
15 information or provide a cyber security plan.

16 So, really for new reactors, the first  
17 opportunity for the NRC to verify compliance of the  
18 cyber security programs is after the combined  
19 license is issued. Which may be long after the  
20 referenced design certification was complete and  
21 for operating reactors, the design information  
22 becomes available for inspection when the system  
23 is entered into the licensee's cyber security  
24 program.

25 So, this timing difference increases

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 the risk the COL holders or licensees who are  
2 ultimately responsible for complying with the  
3 NRC's cyber security regulations will have to  
4 address any vulnerabilities in this design after  
5 the design has been completed.

6 Next please. So, the ACRS has raised  
7 concerns regarding control of access to plant  
8 equipment and networks in which they emphasize that  
9 control of access to critical plan systems should  
10 be reviewed as part of design certification and COL  
11 application reviews. They have also raised a  
12 similar concern regarding the licensing reviews on  
13 operating plant digital I&C upgrades.

14 Next slide. So, the ACRS has  
15 recommended uni-directional communication from  
16 Level 4 to Level 3 and from Level 3 to Level 2 of  
17 the cyber security defensive architecture. That  
18 is enforced via a communication flow enforcement  
19 device and the design of this device would be  
20 reviewed during licensing.

21 So, that slide is a picture of a  
22 recommended approach that is described in Reg Guide  
23 5.71 and previously the ACRS has also raised  
24 similar concerns when Reg Guide 1.152 Revision 3  
25 was updated to remove the cyber security guidance.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           In that case, ACRS believed that cyber  
2 security controls should be reviewed during the  
3 licensing to demonstrate compliance to 10 CFR 73.54  
4 and they did not find that was -- that we should  
5 remove the guidance for cyber security from Reg  
6 Guide 1.152.

7           In addition, the NRC has received  
8 feedback from design certification applicants that  
9 the staff should review cyber security design  
10 features as part of the design certification  
11 application review.

12           For example, GE Hitachi submitted the  
13 ESBWR Cyber Security Program Plan as part of the  
14 ESBWR design certification application.

15           Similarly, Westinghouse submitted the  
16 AP1000 PMS Computer Security Plan.

17           But, since demonstrating compliance to  
18 10 CFR 73.54 is the responsibility of the COL  
19 applicant, staff was not able to review aspects of  
20 the plan addressed in 10 CFR 73.54.

21           And recently, NuScale requested the NRC  
22 review cyber security features as part of their  
23 design certification application that they're  
24 planning on submitting. However, as you can see,  
25 we still run into the same challenges that we would

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 not be able to perform those reviews during  
2 licensing or design certification.

3 So, there are international standards  
4 that recommend that cyber security requirements be  
5 defined as early as possible in a system's  
6 lifecycle. For example, IEC 62859.

7 And we do see that consideration of  
8 cyber security early in the system development  
9 lifecycle can improve both a system's ability to  
10 resist a cyber attack and limit the adverse  
11 consequences of a successful cyber attack.

12 We do want to recognize that some  
13 licensees have worked with vendors to incorporate  
14 cyber security controls as part of the development  
15 of digital I&C systems. However, this is a  
16 voluntary measure.

17 And because design certification  
18 applicants are not required to address cyber  
19 security, we feel all applicants must address the  
20 requirements of 10 CFR 73.54 later during licensing  
21 process and as a result, cyber security controls  
22 are often not considered during the early stages  
23 of system development lifecycles and if a  
24 vulnerability exists within the installed system,  
25 the licensee would have to either modify the system

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 or implement a compensatory measure to mitigate  
2 that vulnerability.

3 And this approach may not be as  
4 effective as developing a more secure and robust  
5 system that's provides inherent protection against  
6 cyber attacks.

7 So, another benefit that we see is that  
8 incorporation of cyber security design  
9 requirements into the NRC's regulation would  
10 enable the NRC to review the applicant's or  
11 licensee's proposed cyber security measures  
12 earlier in the licensing process.

13 So, we see that incorporation of cyber  
14 security design requirements into the NRC's  
15 regulation would enable the NRC to perform  
16 licensing reviews of applicant's and licensee's  
17 proposed cyber security measures earlier in the  
18 process and that cyber security design  
19 requirements will provide an added level of  
20 regulatory assurance for new reactor designs and  
21 for new safety I&C systems to be installed in  
22 operating reactors. In this case, the COL holder  
23 or licensee would be able to reference the staff's  
24 safety evaluation on the cyber security design  
25 controls in their cyber security program.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           For example, if the staff review the  
2 design of an information flow enforcement device  
3 like a data diode during licensing and confirms  
4 that this device provides the unit direction of  
5 communication flow enforcement via hardware means,  
6 then the COL holder and licensee would be able to  
7 reference the staff's safety evaluations to  
8 support subsequent cyber security inspections.

9           We're currently looking at three  
10 potential options to incorporate cyber security  
11 design requirements.

12           The first one is to develop cyber  
13 security design requirements to complement the  
14 current programmatic cyber security regulations in  
15 a more holistic manner. This would be applicable  
16 to both design certification and COL application  
17 as well as licensees seeking approval of digital  
18 upgrades for safety and important to safety systems  
19 and we want to state that although we recognize that  
20 tends to be a part of 73.54 covered systems that  
21 are associated with safety and important to safety  
22 as well as EP and security functions, the design  
23 requirements would only be applicable to systems  
24 that perform safety and important-to-safety  
25 functions. So, we're not looking at all SSEP

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 functions. Only safety and important-to-safety  
2 functions.

3 And also, licensees and applicants  
4 could provide -- we see, you know, that one thing  
5 that's to be provided would be information that  
6 demonstrates that cyber security controls were  
7 considered during the design of systems that  
8 perform safety and important-to-safety functions.  
9 This could be the result of cyber security  
10 vulnerability assessments conducted for systems  
11 and information on how any vulnerabilities  
12 identified are mitigated.

13 Next slide. So, it would be kind of  
14 similar to how SDOE reviews are done, but to address  
15 cyber security to address malicious acts, too.

16 So, the second option is to develop  
17 regulations to require that technical controls for  
18 information flow enforcement be submitted to the  
19 NRC. So, this is a much more limited review. So,  
20 specific to the controls specified in Section B.1.4  
21 of Reg Guide 5.71 which is the one-way,  
22 hardware-based data communication path between the  
23 Levels 4 and 3 and Levels 3 and 2. The cyber  
24 security defensive architecture.

25 So, we're limiting the scope to a much

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 smaller review. It only would be targeted at the  
2 battery devices between the different levels of the  
3 cyber security defensive architecture.

4 Next slide. And, of course, the last  
5 remaining option is just to do what we are doing  
6 right now which is to continue to verify compliance  
7 to the licensees' operational cyber security  
8 program via inspection without first conducting a  
9 cyber security design review of any system.

10 Next slide. So, just to summarize, we  
11 are considering options for incorporating cyber  
12 security design requirements for power reactors.  
13 This effort is continuing to address concerns  
14 raised by the ACRS as well as Design Certification  
15 Applicants.

16 We want to emphasize that the NRC is not  
17 looking to add new cyber security requirements, but  
18 potentially changing the licensing process to  
19 enable us to perform cyber security reviews as a  
20 part of licensing. This is meant to complement the  
21 existing cyber security programmatic requirements  
22 and not change that programmatic requirement.

23 We are currently considering these  
24 three options and we would like to hear back from  
25 industry stakeholders and also, if you have any

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 recommended options that we have not considered.

2 So, can open it up to discussion right  
3 now.

4 (Whereupon, the above-entitled matter  
5 went off the record at 8:54 a.m. and resumed at 9:10  
6 a.m.)

7 MR. JONES: Okay. Welcome back.  
8 Sorry for the technology fiasco here. We're going  
9 to shift over to all handheld mics. So, folk on  
10 the speaker's table here, may sure you use a  
11 handheld mic and in the audience, I'll just bring  
12 you a mic whenever or we'll pass it. One or the  
13 other.

14 Also, please make sure that when you  
15 speak that you give your name and your affiliation  
16 please. Thank you.

17 We're going to start off now with a few  
18 words from Richard Stattel from staff.

19 MR. STATTEL: Thank you. I just  
20 wanted to add a little bit of perspective to  
21 Deanna's presentation.

22 There's really two different dynamics  
23 that are going on with cyber security. One has to  
24 do with the operating plants and that's where I'm  
25 being -- I'm representing that side and the other

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 is the new plants and they're very different  
2 dynamics because the operating plants what we're  
3 finding is they're doing very few modifications.  
4 So, we have very little opportunity to review cyber  
5 security features in the systems or those programs.

6 So, for the operating plants, the  
7 programmatic requirements from 73.54 are really --  
8 we're getting a lot more bang for our buck than we  
9 would get if we were relying on licensing review  
10 activities and on the new plant side, it's kind of  
11 the opposite. Because on the new plants, we're  
12 reviewing designs right now and we're not reviewing  
13 the programs because the programs don't go into  
14 effect until we get the COL applicants involved.

15 So, all those inspections and the cyber  
16 security plan implementations are kind of future  
17 activities. So, what we're trying to do is we're  
18 trying to be consistent between the operating and  
19 new plants and try to cover the gaps because I think  
20 there are gaps or at least perceived gaps. We're  
21 receiving that kind of feedback from ACRS and from  
22 industry and we're trying to fill those gaps and  
23 that's really what this workshop is all about as  
24 far as identifying what the gaps are.

25 I think, you know, the staff has had a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 lot of internal discussions. So, we think we have  
2 an understanding of it, but we'd also like to get  
3 both operating and new reactor perspectives on that  
4 as we go forward today.

5 So, I just want to add that perspective  
6 and background. Thank you.

7 MS. ZHANG: So, did you --

8 MR. BAILEY: All right. My name's  
9 Mike Bailey. I'm with Duke Energy.

10 First off, I want to thank the NRC for  
11 the opportunity to participate in these  
12 discussions about the design for digital I&C as  
13 well as cyber security requirements and processes.

14 We have looked at the information that  
15 was provided as part of this meeting. We had some  
16 discussions within the industry ourselves trying  
17 to better understand and one of the things we wanted  
18 to come out of this with is a better understanding  
19 of the effort that is under way and what we're  
20 trying to address through this effort.

21 We do have several questions to try to  
22 address. Trying to clarify some of our  
23 understanding of what has been proposed or what is  
24 being looked at at this point in time.

25 In the initial discussion and kickoff,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 we talked about the fact, I guess, there's no plan  
2 for cyber security requirement changes as part of  
3 this particular effort. Also, some of the  
4 discussions up here talked about the fact that  
5 we're looking more at process changed.

6 Some of the information in the slides  
7 tended to point towards the fact that we're  
8 actually looking at design requirements or  
9 regulations. So, we're trying to understand what  
10 was actually being proposed in regards to are we  
11 actually looking at design regulations or  
12 requirements or additional digital requirements  
13 that are not currently out there as part of this  
14 effort.

15 MS. ZHANG: We are not planning on  
16 adding any additional technical requirements, but  
17 from a process perspective, we do need new  
18 regulations in order for the NRC to perform the  
19 design review.

20 So, currently, it's programmatic  
21 requirements and as such -- and it doesn't design  
22 certification applicants. As such, any  
23 information that's -- even if it's submitted  
24 voluntarily, we have no means of performing a  
25 licensing review for that.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 MR. BAILEY: And Rich touched on, and  
2 Deanna, you touched you it as well, some of the I  
3 guess areas that you sort of see this gap that we  
4 need to try to cover with these programmatic  
5 changes.

6 One of the things as an industry we had  
7 talked through is between Part 50 and Part 73.  
8 There seems to be a pretty good dovetailing between  
9 what is actually covered in the design  
10 certification piece as well as the programmatic  
11 cyber security area and as a result of that, I mean,  
12 there was even some presentations that had been  
13 done with ACRS back in 2011 on February 23rd with  
14 Jay Amin and Matt Gibson at that time. Covered how  
15 those various requirements and regulations that  
16 currently exist work to insure safety and security  
17 of the existing systems that are being installed.

18 What gaps do we see? And I understand  
19 the process gaps. But do we see any gaps in regards  
20 to regulations that would not insure security or  
21 safety at this point in time with what's currently  
22 being done in the design certification or the cyber  
23 security review process?

24 MS. ZHANG: I think, you know, NSIR can  
25 chime in if what I'm saying is not correct.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           Just to give an example, I guess, we've  
2           seen where design certification applications where  
3           there's a lot of interconnectivity between  
4           different systems, safety, critical -- basically  
5           critical systems and systems that, you know, are  
6           less critical from a cyber security perspective,  
7           but because everything's interconnected in  
8           accordance with Reg Guide 5.71, they would all need  
9           to be protected at the same level and thus from,  
10          you know, when the design certification applicant  
11          made that design, you know, it added -- it basically  
12          required more systems to be protected from a COL  
13          applicant who's going to inherit that design and  
14          as such, you know, there would be more risk involved  
15          or they wouldn't have to modify the design or make,  
16          you know, or protect more systems.

17                 MR. STATTEL: I'll add to that. I can  
18                 speak from the operating plant side again. The  
19                 perceived gap really has to do with the amount of  
20                 attention that we give to cyber security during the  
21                 design review.

22                 So, as you know for the Oconee Reactor  
23                 Protection System design, we actually did perform  
24                 a cyber security review because it predated the  
25                 current policies and the rule. So, there wasn't

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 really any transfer to the program that occurred  
2 during that review.

3 When we presented to ACRS the Diablo  
4 Canyon application, they asked a lot of questions  
5 about the design review and what we were  
6 considering from the cyber perspective and  
7 basically, no, we're not considering that during  
8 our review now, but that will be covered later on  
9 at the time when these systems get implemented into  
10 their cyber security program.

11 So, the way we anticipate that going  
12 forward is the plant or the licensee would identify  
13 the new system as being a critical digital asset.  
14 They would do the assets. They would identify the  
15 security impacts of that and then they would take  
16 those measures. All future tense. Right? So,  
17 the perceived gap is that time frame between when  
18 we do our license amendment review and when the  
19 system actually gets incorporated into the cyber  
20 security program.

21 So, it's a time difference and there's  
22 not a direct turnover from what the staff reviews  
23 as part of the design and what NSIR would be  
24 performing their inspection items for. Okay.

25 So, and I think it's similar, but a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 little different for the new plants and, you know,  
2 I haven't been receiving the same feedback from the  
3 new plants. So, for the new plants, it's different  
4 in that they have really no opportunity because  
5 they're not seeing the detailed designs. Because  
6 a lot of that's deferred to the closure of the  
7 ITAACs and the DACs. So, there's currently no  
8 emphasis on the cyber security aspects.

9 So, the fear is that they do not get  
10 addressed as the design goes forward and then when  
11 the COL picks up that design and takes over and  
12 initiates their cyber security plan, you know,  
13 it'll require new design changes and other like  
14 backward type reviews. Backward looking reviews.

15 So, I think that's more of a risk factor  
16 with the new plants.

17 MS. ZHANG: And from a new plant  
18 perspective, you know, as we had mentioned before,  
19 73.54 does not apply to design certification  
20 applicants.

21 So, there is a much greater timing  
22 difference potentially. So, a design  
23 certification might come in with no COL  
24 applications to come with it. So, they may not be  
25 well informed of the cyber security needs of future

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 COL applicants.

2 MR. HERB: This is Ray Herb, Southern  
3 Nuclear.

4 I'd like to ask a question to clarify  
5 the scope of this proposed new regulation.

6 Currently, Part 50 is very clear on  
7 safety components. It becomes less clear in the  
8 non-safety arena.

9 How is this potentially going to cloud  
10 that issue even further?

11 MS. ZHANG: So, for new reactors, it's  
12 any systems that we would review normally under a  
13 design certification for Part 50.52.

14 We would review those systems if there  
15 are any cyber security controls implemented for  
16 those systems. So, if it's not a system we would  
17 normally review as part of design certification or  
18 COL application review, then we would not do a  
19 review of that particular system.

20 MR. HERB: Okay.

21 MS. ZHANG: And it's something similar  
22 if there's --

23 MR. STATTEL: Yes, let me say a couple  
24 of words on that. That's a very good question and  
25 it's something we've been kind of struggling with.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           Because if I hear you currently, your  
2 concerned that the -- we're expanding the scope of  
3 cyber security review into the non-safety and  
4 important-to-safety regimes. Right? Is that  
5 correct?

6           MR. HERB: Correct.

7           MR. STATTEL: Okay. And there is some  
8 truth to that. So, for example, during the Oconee  
9 review, we did do a design review of the device that  
10 is basically enforcing the one-way communications  
11 from the safety system and that was a non-safety  
12 component of that system.

13           So, I think it's true, you know, that  
14 cyber security really goes beyond just the safety  
15 system. You can't just draw a box around the  
16 safety system and say because -- you know, because  
17 I did this design review or because it's designed  
18 correctly, then it's secure from a cyber  
19 perspective.

20           So, you really have to -- you do have  
21 to expand the scope beyond that and where you draw  
22 the lines, I think that's something that's kind of  
23 up in the air. That's something we really need to  
24 discuss.

25           MR. BAILEY: Staying on the scope

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 topic, just a follow along question with it.

2 We talked about the interconnectivity,  
3 a lot of interconnectivity of digital components  
4 or systems at the plant.

5 Now, the scope part sort of pointed to  
6 new reactors. Things that would be on the NRO  
7 scope. Basically, instrumentation controls that  
8 would be looked at.

9 The examples that Rich provided for  
10 Oconee and Diablo Canyon were safety specific.  
11 Safety system specific.

12 Granted we did go out with a non-safety  
13 device to address one-way communication, but most  
14 of the interconnectivity that you get into is on  
15 the non-safety side where you start getting into  
16 control systems that actually control the plant and  
17 need to share information as well as your plant  
18 computer and plant information systems that  
19 interface information out to operators or to  
20 maintenance and plant engineering personnel.

21 So, from a scope standpoint, most of  
22 your connectivity really happens when it's on  
23 non-safety and I would think things that typically  
24 aren't reviewed for NRO or NRR from a design  
25 certification standpoint.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 MS. ZHANG: And, you know, I think we  
2 need to look into how much would extend into  
3 non-safety systems. Typically, for new reactors  
4 right now, we do look at the control systems.  
5 Particularly when it impacts safety. That would  
6 be our focus, too. But with cyber security as 10  
7 CFR 73.54 defines important-to-safety functions,  
8 there might be a little bit of a difference.

9 So, we will need to reconcile that and  
10 that's something that we would have to look into.

11 MR. STATTEL: Yes, I would just add.  
12 So, for the operating plants, typically, if we're  
13 looking at a license amendment, we really get all  
14 that's in our purview is that safety system.

15 So, it's really impossible to address  
16 all of the cyber security aspects outside of the  
17 context of the installation and all the interfaces  
18 to the non-safety systems. So, I don't think it's  
19 a complete answer.

20 I don't think -- you know, we could  
21 expand the scope of our -- of what we do during the  
22 design evaluations, but that's not going to get us  
23 to where we need to be as far as having assurance  
24 of cyber security. So, it really still has to have  
25 some programmatic aspect.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           So, NSIR still needs to be involved.  
2           They still need to perform the inspections. We're  
3           really relying on the cyber security plans and the  
4           implementation of those plans to provide the  
5           assurance for security.

6           But, at the same time, I think the  
7           technical staff is kind of in agreement. You know,  
8           we believe that we're capable of performing  
9           additional scope of review during our safety  
10          evaluations to kind of help that process along and  
11          give some added assurance.

12          So, I don't think there's any one answer  
13          to that.

14          Particularly in operating plants, I  
15          think that our purview is really limited to the  
16          safety system. So, we really can't go outside of  
17          that. We're not looking at the system in the  
18          context of the installation and all the interfaces.

19          I don't think that's true necessarily  
20          for the new plants. I think they do have the whole  
21          system in front of them. So, they actually do have  
22          a broader perspective on that.

23          MR. BAILEY: And, Rich, on the Ocone  
24          example, I know whenever you all -- we went through  
25          the efforts on the port tap aggregator to do the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 isolation. I didn't necessarily consider that  
2 branching outside the system myself because it was  
3 more or less a -- all the issues we've been talking  
4 about with the safety-related software and how it  
5 dealt with the isolation capacity. That was just  
6 another means to address isolation and so it to me  
7 was actually -- even though it was a non-safety  
8 element, it is still part of the actual system and  
9 requirements for the system. So, I didn't see that  
10 necessarily as a branching out into non-safety  
11 myself too much.

12 MR. HERB: I have an additional  
13 question related to scope.

14 The design requirements for a  
15 protection system are to protect the health and  
16 safety of the public through protection of the  
17 barriers to release of radioactivity.

18 In some cases, some of the cyber  
19 security design requirements make conflict with  
20 that original design purpose of our protection  
21 system.

22 How are you going to handle that if you  
23 incorporate that into Part 50? Those design  
24 requirements and wouldn't it be better to leave  
25 those requirements in 73.54 when the cyber security

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 threat picture often changes as time goes on?  
2 Where the function of the protection system is  
3 static and often remains the same forever and so,  
4 I think you see where I'm coming from. Changes to  
5 the threat vector could impact your design of your  
6 safety system over time if you've incorporated some  
7 of these design factors into the design of your  
8 safety system.

9 MR. PEZESHKI: Okay. The reason why I  
10 wanted to speak first is you had mentioned a  
11 transition from 73 space to 50 space and I don't  
12 believe that is the goal here.

13 The intent is not to generate design  
14 level cyber security requirements to replace the  
15 programmatic requirements. The idea is more or  
16 less to create cyber security design requirements  
17 that will dovetail with the programmatic level.  
18 The idea being that industry can tackle cyber  
19 security concerns earlier in the process to better  
20 meet the programmatic level cyber security  
21 requirements.

22 MS. ZHANG: And even in the current  
23 guidance in Reg Guide 5.71 as well as Reg Guide  
24 1.152, we emphasize that we don't want cyber  
25 security features to adversely impact safety. So,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 performing the safety function has to always come  
2 first.

3 If there are cyber security controls,  
4 not necessarily features, that could be adopted  
5 when you're designing the system to make it such  
6 that it's, you know, less likely that a cyber attack  
7 will be successful or reduces the attack vectors,  
8 then I think that is what we're looking at. You  
9 know, reviewing. Not necessarily that a  
10 particular, you know, like something like an IDS,  
11 intrusion detection system, is implementing a  
12 safety system.

13 So, we definitely want safety -- the  
14 safety function to be the priority.

15 MR. STATTEL: Yes, I sure -- I think  
16 what you said, Ray, is kind of supporting the idea  
17 that we really do need to maintain the programmatic  
18 requirements.

19 I always say that, you know, the safety  
20 systems, these are the crown jewels that we want  
21 to protect. We don't really want to complicate  
22 them and add these measures into them and we've been  
23 working with international agencies. IAEA has a  
24 new safety guide that's out that has guidance to  
25 that effect.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           So, if you're choosing whether or not  
2           to implement a cyber security measure, if you're  
3           choosing whether to implement that on a -- within  
4           a safety system or within a non-safety system,  
5           there is guidance out there and we're also working  
6           with the IEEE 74.32 group to add to -- include that  
7           guidance for the U.S. plants.

8           So, however, the option is still there.  
9           So, if there are measures, if there are Reg Guide  
10          5.71 measures that you choose to implement within  
11          the safety system, I'll use the intrusion detection  
12          not that I would ever expect anyone to put those  
13          kind of features into a safety system, but if you  
14          choose to do that or any of the other measures from  
15          the Reg Guide, the idea that we turn a blind eye  
16          to that, you know, as part of our safety evaluation  
17          review and we rely on the program by itself to  
18          evaluate the impacts of that or the effectiveness  
19          of that, that's kind of what this -- what we're  
20          talking about here. That's what we're trying to  
21          cover.

22                 I think it's beneficial to have the  
23                 technical staff review those features if the  
24                 applicant chooses to implement them in the safety  
25                 system at the time of the safety evaluation. I

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 think that's beneficial because, you know, we're  
2 the ones that would, you know, have the expertise  
3 in that area.

4 MR. GIBSON: I don't think I believe  
5 the --

6 MR. JONES: Again, for all the  
7 speakers, please give your name before you speak.  
8 Thanks.

9 MR. GIBSON: Matt Gibson with EPRI.  
10 Just want a -- a process observation. You look at  
11 this thing technically. Something you should  
12 consider is that a design process involves  
13 tradeoffs. Right? I mean, so you take all the  
14 competing system requirements and you figure out,  
15 you know, how I should do this. Well, one of the  
16 things you want to keep in mind is that from a cyber  
17 security point of view, the designer has a lot of  
18 options to address the cyber security requirements  
19 of 73.54 that are outside the actual design of the  
20 system.

21 So, I think when you think about this  
22 problem think about the sequential timing of when  
23 the design decisions are made. It's true that a  
24 COL applicant or a DCD or vendor has to come up with  
25 at least some level of design to get certified.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           At some point though, those design  
2 decisions are at a certain point in time in the  
3 design certification. Later on when a COL  
4 applicant adopts that, one of the things they have  
5 to do is continue that process by evaluating that  
6 design against their chosen cyber security  
7 programmatic implementation requirements.

8           The point I was going to get is let's  
9 keep in mind that some of this has a timing -- from  
10 a technical process point of view, there's a timing  
11 concept and design process that you could disrupt  
12 if you go too far with trying to move some of these  
13 topics at different places in the design sequence.  
14 It can have an unintended consequence and that's  
15 just a comment I want to bring to the table.

16           MR. JONES: Other comments?

17           MR. STATTEL: Yes. I do agree with you  
18 and, you know, I think a lot of this falls back to  
19 engineering judgment, but the fear that we have and  
20 when the decision was made to basically shift  
21 reliance onto the programs, I had a concern that  
22 even back then, you know, six/seven years ago, that  
23 the inspection teams that were looking at these  
24 cyber programs wouldn't necessarily have the  
25 technical background to be able to review the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 impact on the designs and that's where the concept  
2 of the SDOE came from.

3 So, when we do our technical reviews,  
4 you know, we're looking for if you've implemented  
5 any of these cyber measures, we want to have some  
6 assurance that it doesn't have any adverse impact  
7 on the safety function.

8 So, we have some competing objectives  
9 here. So, one of the things is we want your safety  
10 systems to be as simple as possible. We only want  
11 them to do functions that are safety functions and  
12 on the other side, we have these cyber security  
13 requirements that are saying make the system more  
14 complicated by added cyber security functions.  
15 Right?

16 So, you know, the decisions get made at  
17 various points during the design process. We just  
18 want to make sure if the decisions are made early  
19 enough and we have that opportunity during the  
20 design reviews to evaluate those designs, that we  
21 don't miss that opportunity. Because if we simply  
22 defer everything to the inspection teams, I think  
23 there's a risk or there's a danger of things falling  
24 through the cracks.

25 So, people will implement cyber

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 security measures that don't get evaluated. They  
2 don't get properly assessed for impact on the  
3 safety functions and, you know, we could have  
4 problems down the line without having had those  
5 design reviews done up front.

6 Now, SDOE was intended to address that.  
7 How well it does that, you know, I guess that's,  
8 you know, a matter of, you know -- there are  
9 different cases that you could study.

10 MS. ZHANG: Just very quickly. We're  
11 not looking at implementing everything within Reg  
12 Guide 5.71 or NEI 08-09. This will be selective  
13 maybe controls that could be considered earlier and  
14 this is more about a consideration of them. Not  
15 necessarily implementing those controls and  
16 definitely, you know, if you had to implement it  
17 within the safety system, I think that a lot more  
18 attention needs to be paid for that.

19 We do see a hand off between the design  
20 certification applicant and the COL applicant.

21 Now, you know, we -- it's not like  
22 everything can be done by the design certification  
23 applicant, but if there's something they can do to  
24 kind of -- it's a look ahead to enhance the security  
25 of their design, I think that could be done earlier

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 and I think that would make it a little bit better  
2 for the COL applicant.

3 MR. STATTEL: One other point. As  
4 Deanna mentioned, we've had several design  
5 certification applicants submit cyber security  
6 plans or documents, licensing documents and the  
7 fact that they are able to create those documents,  
8 you know, clearly it's kind of a -- kind of  
9 testifies that there are certain cyber security  
10 measures that they're incorporating into their  
11 designs at the early stages. Which is a good  
12 thing.

13 And the fact that our process doesn't  
14 really allow us to review that and credit that in  
15 those advance stages, kind of points to a problem  
16 and I think that's where the ACRS' concerns are  
17 really coming forward.

18 MR. GROSS: I have a process question.  
19 Is there sort of a time horizon you're working to  
20 for the SECY paper? Do you have a, you know,  
21 commitment to the Commission to get something to  
22 them by a certain date?

23 MS. ZHANG: We don't have a formal  
24 commitment to the Commission, but we are looking  
25 at completing it by the end of September.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 MR. GROSS: Do you expect that there  
2 would be additional public workshops to discuss the  
3 progress and the development of the SECY paper  
4 before September?

5 MS. ZHANG: Well, you know, if that's  
6 something that the industry would like, we could  
7 definitely set that up.

8 MR. JARRETT: I guess I'd like to -- Ron  
9 Jarrett, TBA.

10 Rich, you mentioned Diablo Canyon  
11 review. We've discussed 74.32, NUREG 1.152. In  
12 those documents, there is cyber-related or  
13 security-related requirements.

14 So, I assume when you did Diablo review,  
15 you looked at those areas.

16 MR. STATTEL: Not really cyber  
17 security. So, our review is really limited to the  
18 secure acknowledgement and operating environment.

19 MR. JARRETT: Secure. Yes.

20 MR. STATTEL: So, I guess -- you know,  
21 our review guidance doesn't have the word cyber in  
22 it.

23 MR. JARRETT: I understand, but  
24 there's a lot of aspects in that. There's some  
25 aspects in 74.32 that do touch on it and I guess

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 I'm trying to get a feeling of what additional  
2 things -- you know, there's -- we've improved  
3 74.32, 2010 added more requirements that were in  
4 the original Reg Guide Rev 2 and now, we're out to  
5 -- with a new version of 74.32 that even expands  
6 that area. So, I'm trying to see -- get a feeling  
7 of what additional things would be reviewed in  
8 addition to what's in that document.

9 MR. STATTEL: Okay. There's two  
10 different scopes at hand here. One is the scope  
11 of IEEE 74.32 which goes beyond what our review  
12 scope for our safety evaluations is. Our intent,  
13 because right now kind of the guidance is kind of  
14 duplicated in the Reg Guide and in the IEEE  
15 standard, these changes we're currently making to  
16 the IEEE standard make it consistent, and Deanna  
17 can speak to this, too, make it consistent with our  
18 current Reg Guide review criteria.

19 Our plan is the next revision of Reg  
20 Guide 1.152 would basically delete that section and  
21 we would simply endorse the IEEE standard for the  
22 SDOE aspects.

23 We do -- right now, until we get some  
24 direction from the Commission and that's kind of  
25 the purpose of this paper here, our policy is really

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 to limit the scope of our review to SDOE.

2 So, in other words, we're not ignoring  
3 the cyber security requirements. But, again, the  
4 SDOE perspective is if cyber security measures are  
5 being put into the design, we are evaluating  
6 whether those features have any impact on the  
7 safety functionality of the system. So, our  
8 safety evaluation is still focused on safety.  
9 Okay.

10 So, it's a little different  
11 perspective.

12 MS. ZHANG: So, for the SDOE review, I  
13 just want to remind everyone that it's focused on  
14 addressing non-malicious acts.

15 So, if there is anything that, you know,  
16 was there to address malicious aspects, too, we  
17 cannot make a judgment as far as the -- you know,  
18 whether it could be used to address malicious acts.  
19 Our safety evaluation would only consider to  
20 address non-malicious acts.

21 MR. JARRETT: Just a follow-on  
22 question. When we worked on ISG4, it was to allow  
23 two-way communication safely. In essence, it was  
24 kind of like a data diode, but with two-way  
25 communications. You weren't -- if you implement

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 that, you should not be able to affect the safety  
2 system. You know, that's been relevant to the  
3 74.32 and so, where is that headed in this area?

4 MS. ZHANG: Well, what we want to -- you  
5 know, so, we do recognize that a lot of things that  
6 we do for safety could also be used to address  
7 security, but it's not necessarily a complete  
8 overlap.

9 So, you know, although some things can  
10 be used to credit -- you know, to address cyber  
11 attacks, too, but doesn't necessarily mean that  
12 that's the only thing that would be effective at  
13 addressing all cyber threats.

14 So, that's why you do need the  
15 programmatic aspects, a cyber security program in  
16 addition to whatever we do for our safety review.

17 MR. PEZESHKI: And also since during  
18 the SDOE review malicious acts are not considered,  
19 none of that can be referenced or credited for the  
20 eventual programmatic 5.71 or 73.54 review. So,  
21 as I said, one of the hopes here is that this will  
22 give the industry an earlier bite of the apple for  
23 ultimately meeting their 73.54 requirements.

24 MR. REBSTOCK: I'm Paul Rebstock from  
25 the Office of Research. I was involved in the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 development of ISG4.

2 And the bidirectional communication  
3 that that allows is extremely limited and I am not  
4 sure that it's fully appreciated just how limited  
5 that is.

6 That process allows for the non-safety  
7 system to send some data to the safety system which  
8 the safety system can then read and figure out what  
9 to do. It explicitly does not allow the non-safety  
10 system to send any commands to the data -- to the  
11 safety system. It can send a number and the safety  
12 system can be programmed that if that particular  
13 number has a certain value, then it can go do  
14 something that's already been programmed. But  
15 there is no way to send a message into the safety  
16 system that would cause the safety system to do  
17 something unexpected.

18 So, some of the systems that I've seen  
19 under development don't do that. They seem to  
20 think that they're following ISG4, but they allow  
21 commands to be submitted into the safety system and  
22 I think there's some confusion there.

23 MR. GROSS: Hi. This is Bill Gross  
24 from Nuclear Energy Institute.

25 And I feel compelled to tell a story

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 about cyber security in the early days and I got  
2 involved in IT in about 1995 and at that time, it  
3 was -- cyber security in IT was a bit -- it was  
4 the wild, wild west. It kind of still is, but it  
5 was really bad then.

6 And I would imagine for those of you  
7 that had been at that game at that time, you  
8 remember Windows 2000. The most secure operating  
9 system every built. That was the vendor claim.

10 So, let's assume at that time two things  
11 happen. First, Microsoft paid an awful lot of  
12 developers an awful lot of money to be able to make  
13 that claim and those costs were passed on to the  
14 purchaser of the product.

15 Second, suppose that NRC had endorsed  
16 the safety and security features of that at that  
17 time. Right.

18 Now, roll the camera forward 20 years  
19 and you take a Windows 2000 box out of the -- you  
20 know, out of the box it comes in. It's no longer  
21 the most secure operating system ever built.  
22 Right.

23 The licensee who's now purchased this  
24 thing has to install it and build an operational  
25 program to secure it. So, now not only are they

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 paying for the vendor to have built a product that's  
2 not secure because time has gone by, but now they  
3 have to build the operational program that we're  
4 currently required to build to protect it. All  
5 right. So, the costs are being incurred twice for  
6 the same level of cyber security. All right.

7 So, there is a gap as Rich pointed out  
8 between when the NRC approves the design of a system  
9 and when it's built into an operational program.

10 But I would claim that even if that  
11 device was secure at the time that it was certified  
12 because of the emergence of and the changing nature  
13 of the cyber threat and our understanding of the  
14 ability to exploit systems, it's not secure by the  
15 time you install it and you still need the  
16 operational program to do it.

17 I think, you know, another point is if  
18 you claim that if we can't review cyber security  
19 features at the time that it's designed or we don't  
20 have the capability to do that and that limits our  
21 ability to understand how we can secure it when  
22 we're -- you know, when we're going to put it into  
23 operations, really calls into question whether or  
24 not we have the capability to implement 73.54 to  
25 protect the plants that we have today that are

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 replete with digital systems both non-safety and  
2 in the balance of the plant that were never designed  
3 with cyber security features integrated into them.  
4 All right.

5 So, while I appreciate as having, you  
6 know, two degrees in computer science the deep  
7 desire to integrate cyber security features into  
8 the design of systems, it's a temporary -- it's a  
9 temporary fix to a problem that gets bigger and  
10 harder over time and, you know, as was pointed out,  
11 if simplicity is an attribute of safety, simplicity  
12 is also an attribute of security.

13 I've never seen a complex system  
14 adequately protected against cyber attack.

15 So, if you want to protect something  
16 against cyber attack, whatever it is you're trying  
17 to protect should be as simple as possible. Makes  
18 it much easier to do.

19 MS. ZHANG: We appreciate that remark  
20 there.

21 We don't see this as -- that any review  
22 we do for safety or important-to-safety system as  
23 the end all. That this is going to be a completely  
24 secure system.

25 There are going to be additional

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 measures that's going to have to be implemented on  
2 a programmatic level because of evolving threats  
3 and so, what we want -- what we hope to accomplish  
4 is that if they do choose, if a design certification  
5 applicant or a vendor does choose to kind of  
6 consider cyber security earlier in the progress and  
7 they want to have the NRC review those particular  
8 measures that there is a means for them to do that.

9 But, of course, you know, that doesn't  
10 remove the fact that we still need a cyber security  
11 program to address evolving threats.

12 MR. STATTEL: I mean, I guess part of  
13 the workshop here, one of the main objectives is  
14 to kind of solicit feedback.

15 Is there -- I'm not hearing a lot of  
16 resistance or push back on the idea of us performing  
17 these types of reviews during the design  
18 certification process or during the license  
19 amendment review process. I mean, am I incorrect  
20 in that assessment?

21 MR. GROSS: Yes.

22 MR. STATTEL: Okay. That's what I  
23 want to hear. I want to hear, you know, the push  
24 back. I'm really -- you know, the discussion's  
25 kind of gone around in circles here and we're talked

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 about two-way communications and we've given a lot  
2 of good examples.

3 So, I think a lot of us understand, you  
4 know, what the problems are, but we really need to  
5 decide on a path forward for our regulations. How  
6 we go forward and regulate and insure security of  
7 these systems. So, I guess I want to get us back  
8 on track as far as getting that feedback from the  
9 industry.

10 MR. BAILEY: I think Brad wants to say  
11 something and then we'll actually address directly  
12 your question or comment.

13 MR. YEATES: Yes. My name is Brad  
14 Yeates with Southern Company.

15 So, I'm not going to give you that push  
16 back just yet. I'll let somebody else do that, but  
17 I did -- I think you're not hearing it yet because  
18 we're still trying to understand and really, really  
19 seeking to understand. So, my question is still  
20 along those lines.

21 So, what I have heard is kind of two  
22 different perspectives or there's two objectives  
23 you're trying to accomplish.

24 The first one I think is very consistent  
25 with the safety evaluation and that is if an

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 applicant -- a design certification applicant or  
2 a COL applicant chooses to implement cyber security  
3 controls into the design of a system, you want the  
4 ability to review those controls to insure that  
5 they do not have an adverse impact on the safety  
6 function and that makes perfect sense.

7 And I would submit that you have that  
8 authority today. That is part of the safety  
9 evaluation.

10 So that you would not need additional  
11 rulemaking to assert that, you know, jurisdiction.

12 MR. STATTEL: And I agree with that.

13 MR. YEATES: Yes. Now, the other  
14 aspect that I'm hearing, I'm hearing mostly from  
15 Deanna, is that you're seeking the opportunity  
16 earlier in the design process, in the time frame,  
17 to require the implementation of cyber security  
18 controls in the design.

19 And I think that's the area where, you  
20 know, we need more understanding of really what  
21 does that look like. You know, where is that?  
22 What we've seen in the presentation is focused  
23 mostly on the isolation aspect. But there's, you  
24 know, in the Reg Guide 148 -- or yes, 148 or 146  
25 controls --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 MR. STATTEL: I think an example would  
2 serve us well at this point. So, let's pick a  
3 really simple example that a system developer wants  
4 to have a password protection feature in their  
5 system. Right? So, and we've seen these systems.

6 So, we could review that during the  
7 design evaluation and we could say okay, we can  
8 enter different passwords, enter incorrect  
9 passwords, make sure they don't work, but that  
10 doesn't really give us any real assurance that the  
11 system is secure because how they control that  
12 password, how they share it, you know, with their  
13 staff members when the licensee gets the system is  
14 really -- that's -- you know, if they just put it  
15 on their public website and give everybody access  
16 to it or they make the password a non-strong  
17 password, it's just 1, 2, 3, 4, then they're really  
18 not accomplishing that security objective.

19 But what I can do during the safety  
20 evaluation is I can look at the lines of code or  
21 I can look at that actual design features and I can  
22 look at the testing that was done on that and I can  
23 get that assurance like you say that nothing --  
24 entering the incorrect password isn't going to  
25 prevent the safety system from tripping the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 reactor. Okay.

2 And that's that assessment we currently  
3 do. So, we're already doing that. That's  
4 correct.

5 Now, I don't -- I think requirement is  
6 not really what we're after here. We're not -- to  
7 ask me, the technical evaluator, to make an  
8 assessment of whether that password protection is  
9 going to maintain the security of that system  
10 without knowing what the licensee's going to do or  
11 how they're going to control passwords, that's  
12 asking too much of me.

13 But you have the option, I think. I  
14 think if the applicant is willing to put those  
15 measures in place, I guess there's some degree of  
16 assurance that can be achieved as long as you put  
17 the right condition. So, you can establish the  
18 rules for setting that password. You can  
19 establish limits on what the password can be or how  
20 it can be disseminated.

21 So, I think what we're trying to do is  
22 give you the option. Right. So, like we said  
23 before, you know, we already have applicants,  
24 design certification applicants, that want to put  
25 those types of measures forward, but we're really

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 not set up. Our processes aren't really set up to  
2 do the cyber evaluation part of that. We're only  
3 set up to do the SDOE evaluation.

4 MR. YEATES: So, if I were to restate  
5 that, repeating back what I'm hearing, you're  
6 seeking the authority then during the design review  
7 to certify compliance with 73.54 or at least  
8 aspects of it.

9 MR. STATTEL: I guess I'm going to let  
10 the -- see we -- right now, we don't have the  
11 authority to do that in the safety evaluation  
12 processes. So, I guess I'm going to defer to NSIR  
13 to answer that question.

14 MR. FELTS: Yes, I tried to -- Russ  
15 Felts, Deputy Director, Cyber Security  
16 Directorate.

17 As we started off the meeting, I tried  
18 to have the early stage dispel the potential for  
19 that interpretation. That what we're looking to  
20 do is a review that would establish compliance with  
21 73.54 at the design cert stage because 73.54  
22 requires an operational program and so, there's so  
23 much more that needs to be done that would be  
24 impossible to accomplish at the design cert stage  
25 in order to meet 73.54.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 We are --

2 MR. STATTEL: I think it's more  
3 intended to set you up so that it would be easier  
4 for you to complete that certification.

5 MR. FELTS: Easier to complete and more  
6 importantly not impossible to complete. Right.  
7 We don't want a design sitting on the shelf that  
8 is so potentially interconnected or has features  
9 that make it virtually impossible to meet the  
10 programmatic and performance requirements in  
11 73.54.

12 MR. STATTEL: Right. So, reverting  
13 back to our example, if I have done an evaluation  
14 and I have reviewed the password protection feature  
15 not only from a safety perspective, but from a cyber  
16 perspective in terms of how those are controlled,  
17 what measures are put in place to control that, we  
18 can document that and that becomes information that  
19 the inspector that's inspecting your cyber  
20 security program can use to verify that those  
21 measures are being appropriately implemented and  
22 it would -- you know, I think the idea is that would  
23 go a long way towards achieving the certification  
24 that you need to get.

25 MR. FELTS: Yes, and again, I think

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 it's important for us to have this conversation  
2 we're having right now keeping in mind the options  
3 that -- potential options that we laid out. Right.

4 Option 1 would be to review at the  
5 design cert stage the application to verify that  
6 the licensee or the applicant has considered cyber  
7 security. It's very high level. Essentially to  
8 verify that they haven't designed a system that  
9 can't be secured. I mean, that's really  
10 ultimately what we're talking about.

11 Option 2 is verifying that the design  
12 incorporates an architecture that limits  
13 communication at certain levels to enable that  
14 defense in depth requirement in 73.54 to be met.

15 And then Option 3 is the no action  
16 option.

17 And as we said at the beginning of the  
18 meeting, we are seeking input here. If the  
19 industry or others, other stakeholders, have ideas  
20 on other options we should consider, we're  
21 interested in your input.

22 MS. ZHANG: Yes, and also, you know,  
23 for the -- just the password example, we could look  
24 at the design of that feature and say, you know,  
25 if you claim it's, you know, a ten-letter password,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 we can verify it's a ten-letter password, you know,  
2 and that it would only accept a ten-letter  
3 password.

4 Stuff that's really on the design side.  
5 Not how effective it is at protecting a cyber  
6 threat.

7 MR. STATTEL: This also goes back to a  
8 lesson we learned with the Oconee review. So, as  
9 I mentioned before, when we did the Oconee review,  
10 our intention was to perform a cyber security  
11 cyber-based review as a part of the design  
12 evaluation.

13 And what we found was we really weren't  
14 able to get any kind of high assurance that the  
15 system would be secure once it went into operation  
16 because there was too much that had to happen during  
17 the installation and there was too many things that  
18 the licensee -- we were relying on the licensing  
19 to do in order to establish the security of that  
20 system.

21 So, if you look -- if you read the Oconee  
22 safety evaluation, there's a section in there  
23 called -- I believe it's recommended inspection  
24 items. So, we realized that we were not going to  
25 be able to complete our cyber security evaluation

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 during the design evaluation. So, we kind of  
2 kicked that over to the inspectors and they  
3 followed up during the installation and during the  
4 start-up testing and they were looking at what the  
5 licensee -- what measures the licensee was taking.  
6 Locking keys, password protection, controlling USB  
7 ports, things like that.

8 And so, I mean, that was our really only  
9 recourse there. So, we kind of pushed that out to  
10 the inspection space anyway.

11 So, I think we're really talking about  
12 a similar type of turnover and feed forward program  
13 between the safety evaluation -- we want to  
14 communicate with NSIR. We want to communicate  
15 with the future inspectors who are going to be  
16 evaluating the cyber security programs. So, you  
17 know, we want to have that early on understanding  
18 of the design.

19 MR. YEATES: Yes, and this is Brad  
20 Yeates.

21 So, just a matter of making sure that  
22 it's on the record here, too, the process that we  
23 went through for the COL application for the AP1000  
24 at Vogtle 3 and 4, we were required to submit our  
25 cyber security plan along with that COL application

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 so that that plan was -- received a safety  
2 evaluation.

3 Now, the vast majority of plan is  
4 programmatic in nature, but there is one aspect  
5 that is technical design in nature and that was the  
6 defensive architecture. So, within that plan, we  
7 laid out a relatively detailed architecture that  
8 described the communication of functions within  
9 the plant and that was reviewed and approved early,  
10 very early in the design process.

11 So, I would just submit that there  
12 currently is an early design review of that  
13 technical aspect of the cyber security design that  
14 is part of the Part 52 licensing process.

15 MR. JACKSON: This is Terry Jackson  
16 with NRC.

17 So, just to go along with some of our  
18 experience with AP1000, I remember they did submit  
19 to us sort of the cyber security plan and so forth.  
20 I remember the discussions we had with them as it  
21 was in -- it was mixed in with the I&C design  
22 information as well.

23 We ended up requesting that  
24 Westinghouse take that -- the cyber security  
25 information out. The reason was because the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 staff, the I&C staff, couldn't make a call whether  
2 it met 73.54 or not and we couldn't leave it in there  
3 either because we didn't want someone to think it  
4 was some sort of tacit approval if it was left in  
5 there and nothing was said about it. So, they  
6 ended up having to remove that information.

7 Now, in the cyber security plan review,  
8 they may have reviewed some design aspects to a  
9 certain degree, but it's probably at a higher  
10 level.

11 I think overall when the staff was  
12 working on, you know, this SECY paper -- and I think  
13 one thing to understand is that, you know, we're  
14 talking about different kinds of design controls  
15 and stuff. We haven't really sat down and  
16 identified which ones may be in the scope and which  
17 ones may not be in the scope at this time.

18 We felt it was fairly premature because  
19 we wanted to go to the Commission and see do they  
20 even want us to go here before we expend a lot of  
21 resources on it.

22 Now, in the back of our heads, I think  
23 there were some things that we thought would be  
24 beneficial and we thought well, maybe the industry  
25 may think that this will add to efficiency. So,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 for example, we talked about the secured  
2 development and operational environment reviews  
3 that we do in the safety review and we go through  
4 and look at that process.

5 Now, it's very similar to probably like  
6 the vulnerability assessments and stuff that are  
7 done on the cyber security end. So, they look  
8 similar and we -- you know, we were thinking well,  
9 if we're doing this and then later on, someone else  
10 is going to go out and inspect the same thing, but  
11 look at it from a malicious standpoint, is there  
12 a possibility for efficiency in combining the two  
13 and do that up front?

14 So, I think that's kind of the thoughts  
15 we had. We didn't necessary have a concrete idea  
16 as to what kinds of design controls may go in here.  
17 If the Commission gives us direction later on and  
18 say you got to do this, that's kind of like a phase  
19 two afterwards.

20 MR. STATTEL: I'm hearing a little  
21 mixed message here though because I've heard from  
22 industry. So, for example, ESBWR submitted a  
23 cyber security plan. My understanding is that  
24 they did not -- the NRO did not perform a safety  
25 evaluation of that plan or issue a safety

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 evaluation of that plan. Now, AP1000 preceded  
2 that. So, they might have -- that might have been  
3 done prior to the current policies becoming --  
4 going into play.

5 So, you know, because the feedback that  
6 Deanna pointed out is that the design certification  
7 applicants want to submit plans and want to get  
8 safety evaluations performed by the staff and the  
9 staff's unable to do that, but then you're telling  
10 me the AP1000, that's exactly what had happened.  
11 So.

12 MR. JACKSON: I think that was under  
13 the COL applicant versus the design certification.

14 MR. STATTEL: Okay. Okay.  
15 Understood. Okay.

16 MR. BAILEY: I guess we've had a lot of  
17 discussion here and it's been very beneficial and  
18 fruitful to what we were looking at from our  
19 industry discussions that we had prior to the  
20 meeting.

21 Sort of summarizing all the pieces that  
22 you heard and Rich, this goes back to sort of, I  
23 guess, your request for some feedback in regards  
24 to the various options and we felt as an industry.

25 As I noted earlier, definitely

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 appreciate the opportunity to be involved and have  
2 these discussions now with the NRC.

3 One of the things, like I mentioned  
4 earlier, we did have some questions. We had an  
5 initial opinion based on what we saw in the  
6 presentation and so, we had some questions to try  
7 to understand and clarify that and really  
8 appreciate the information that you all provided.

9 As a result of our initial review and  
10 the feedback through these questions and answers  
11 at this point in time and it sort of is a summary  
12 of what all's been presented between the efforts  
13 that currently exist with Part 50 and the efforts  
14 that exist in Part 73, as an industry, we prefer  
15 at this point in time Option 3 that currently has  
16 the fact that there's no additional actions needed  
17 because the current regulations cover what is  
18 needed to insure a secure and safe operating plant  
19 in regards to digital and cyber security.

20 That being said, we definitely still  
21 would be interested in further discussions or  
22 additional opportunities as Bill noted to be  
23 involved in further dialogue to try to see are there  
24 other options out there. We were basically just  
25 looking at Option 1, 2 and 3 and didn't have a lot

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 of time to really factor in what are all the other  
2 options. What are some, you know, scope and  
3 boundary type aspects that could be tied to this?

4 Some of the other -- just to reemphasize  
5 the points that have been made, the items to support  
6 Option 3 and why we feel as an industry we are  
7 providing a safe and secure method by going with  
8 Option 3 is that Options 1 and 2 at this point in  
9 time don't substantially provide anything  
10 additional that's outside of Part 50 or Part 73  
11 design and cyber security program aspects that  
12 would increase or enhance safety and security  
13 beyond what's already being done at the facilities  
14 themselves.

15 Part 50 covers the safety design  
16 review. There's a lot of industry guidance out  
17 there and standards that actually insure that  
18 things are safe and the right equipment is  
19 installed with the right controls and then Part 73  
20 insures that we've got a secure platform and secure  
21 program at the operating units.

22 Also, the licensees themselves, one  
23 option in here is to do one-way transmissions as  
24 part of the cyber security program activities as  
25 well as the new operating reactors cyber security

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 programs. Data diodes or isolation devices are  
2 already factored into the designs. So, from that  
3 standpoint just having additional requirements or  
4 policies in place wouldn't change anything that's  
5 currently already in the system or in the programs  
6 that we have at this time.

7 As far as the burden, this sort of  
8 alludes to some of the things that Bill touched on.  
9 The aspect of including it, paying for it as part  
10 of the design and then paying for it again as part  
11 of the efforts of 73.54 programmatically. We're  
12 not really seeing a potential to reduce the burden,  
13 but we're actually seeing the potential to increase  
14 having to deal with it twice as we go through the  
15 reviews and the program implementation aspects.

16 And then the last point from a summary  
17 standpoint is that at this point in time and the  
18 framework that we have both for new reactors as well  
19 as current operating reactors, we're not seeing a  
20 major gap where we're actually having designs that  
21 are insecure, designs that do not factor in safety  
22 as well as through the design reviews that had been  
23 done and also through the inspections that are  
24 being addressed at this point.

25 So, in summary, that would be the -- I

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 guess, the feedback overall from the industry and  
2 that is based on the initial review and just the  
3 questions that we had, but we are open to additional  
4 discussions.

5 MR. HERB: Again, I'd like to  
6 reiterate. This is Ray Herb, Southern Nuclear.

7 When we say industry, we are talking  
8 operating fleet and not the vendors and the -- I  
9 mean, the design review applicants potentially.

10 MR. BAILEY: Thank you.

11 MR. JUNG: Ian Jung with the New  
12 Reactors.

13 Thanks for the feedback. That's  
14 exactly the purpose of this workshop. Is to get  
15 the industry feedback.

16 Terry Jackson and I are in New Reactors.

17 I just want to share a couple of points  
18 for more targeting new reactors and defense  
19 reactors. Okay.

20 For Option 1, it's three/four years, I  
21 mean, that we have gone through internally as well  
22 as externally with the ACRS and some of the  
23 applicants.

24 There are multiple letters written on  
25 kind of broad ACRS concern regarding the two

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 aspects of this whole licensing versus inspection  
2 framework of the cyber security. ACRS has  
3 specifically wrote letters regarding their desire  
4 and recommendation that cyber design element  
5 should be reviewed in licensing -- at the licensing  
6 stage with the right expertise. That was one  
7 concern.

8 So, I think the staff has taken at the  
9 office level -- through office level discussions  
10 that there were multiple options and one of them  
11 was a rule about any terms of inspection element  
12 that that has implemented in a joint expertise --  
13 inspector -- inspection staff jointly is, you know,  
14 participating in inspection activity, That's  
15 ongoing.

16 There was a sort of a background that  
17 led into this potential option. When the ACRS  
18 spoke to the Commission about their concern on this  
19 broad brush of licensing versus inspection, the  
20 Commission was silent on it. So, I think ACRS  
21 eventually kind of gave up on raising additional  
22 concerns on that.

23 Option 2 became more of a bigger issue  
24 for ACRS last two or three years. Wrote actually  
25 multiple letters. Okay. One for mPower DSRS.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 Difficulties on this standard. IEEE -- I think  
2 IEEE Standard 603 briefing to the ACRS as well as  
3 Office of Research plan. I think there was another  
4 letter.

5 And for Option 2 to consider at least  
6 for practicality perspective is -- is for South  
7 Texas and other applicants and US-APWR as well,  
8 they ended up voluntarily addressing it to address  
9 ACRS concerns to get their license -- licensing  
10 application approved.

11 So, in reality, South Texas operating  
12 records already have those diode air gap measures  
13 in place for those boundary devices. So,  
14 practicality-wise, I see either -- the reason we  
15 couldn't go back to ACRS, don't worry about it.  
16 It'll get done under programmatic element down the  
17 road. They simply didn't like that answer.

18 They started -- ACRS, I think, provided  
19 that recommendation that we could within current  
20 framework interpret the certain regulation in such  
21 a way this element can be part of the staff guidance  
22 that we can modify and review under IEEE 603 and  
23 other elements.

24 So, I think -- so, right now, we are in  
25 a stalemate with ACRS on that. So, we'd like to

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 hear potentially or consider for the industry for  
2 new reactors and defense reactors to have that very  
3 narrow element to be something that we can put it  
4 in the books so that we don't have that stalemate.  
5 Because technical solution not only cannot do it  
6 and then actually empower NuScale and South Texas  
7 MHI. They all have no problem doing -- specifying  
8 that element as a part of the licensing now.  
9 Right.

10 So, Option 2, I want the industry to  
11 consider that element. Otherwise staff and  
12 applicant as well as ACRS will I expect to continue  
13 to have this unnecessary significant burden on --  
14 going back and forth on that. I think it's going  
15 to still continue to come to the Commission level  
16 on this issue for a while. So, I'm just suggesting  
17 that to consider.

18 So, one last item is on the defense  
19 reactor policy statement of the 2008. Yes, the  
20 Commission -- there's one element regarding cyber  
21 security element where it's a policy set up in such  
22 a way that these -- among all the other features  
23 simplicity and all the easy to analyze, easy to  
24 approve licensing predictability and stipulate and  
25 all that. There's one element also includes a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 cyber security and overall plant system design that  
2 are developed from the get go so that it minimizes  
3 the implementation challenges. There's some  
4 language to that.

5 So, sooner or later, it seems like we  
6 need to reconcile that policy against the real  
7 practice that's happening. It seems like policies  
8 that you have to design it's sort of inherently safe  
9 and secure design in the policy. But the practice  
10 we are doing right now, it might be okay. That's  
11 what you're thinking, but maybe we can continue to  
12 have a dialogue on maybe longer term future. That  
13 is policy versus real practice and hopefully, it's  
14 more economic or more logical since we need to  
15 consider that all the way.

16 I just want to share those thoughts.

17 MR. CLARKSON: Greg Clarkson with  
18 NuScale Power.

19 I'd like to pause a moment and consider  
20 the scope of what we talked about today. We've got  
21 new plants, existing plants, protection systems,  
22 monitoring and indication systems, control  
23 systems, corporate networks, a secure development  
24 environment, how they're developed, how they're  
25 deployed into the plant, the programmatic aspects,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 design attributes. This is a lot.

2 And I've heard a lot of examples and a  
3 lot of the examples are very specific to a  
4 situation. My concern is, and I think maybe this  
5 is the concern I'm hearing, there is no single  
6 answer to this whole scope of what we're  
7 discussing.

8 So, some of the examples that Rich  
9 brought up on specifics of safety system design,  
10 that's where I'm at with what I'm doing with NuScale  
11 Power. I'm designing a reactor protection system.  
12 That the priority is to design a protection system  
13 that is safe, protects the health and safety of the  
14 public period.

15 In the design of that protection  
16 system, we identify hazards and we design a system  
17 to mitigate those hazards. Part of that design  
18 evolution is to consider malicious and  
19 non-malicious hazards, cyber whatever you want to  
20 call them. The black box doesn't know any  
21 different. How can it be defeated? How can the  
22 safety function be defeated whether it be malicious  
23 or non-malicious? So, it's a hazard.

24 We design mitigation strategies. We  
25 change the design. We sometimes live with the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 hazard because the effect of a hazard is tolerable.  
2 But, at any rate, it's a hazard.

3 As it stands now, my understanding, and  
4 when this took effect in 2009 time frame, put into  
5 regulation in 2011, the staff was asked not to look  
6 at, one, aspects of these hazards if they are  
7 malicious cyber hazards. That makes no sense to  
8 me.

9 Because as a designer, I'm considering  
10 it as a hazard. The staff is reviewing that at that  
11 level of detail while the design is being -- well,  
12 somewhat shortly after the design has been made.

13 The level of knowledge and the level of  
14 detail and the level of review effort to get down  
15 to that level is so -- is such a burden, why not  
16 do it at that time?

17 So, from that perspective, it makes a  
18 lot of sense to me for -- I don't know if it's Option  
19 2. I've lost track of the options. But, Option  
20 1. Okay.

21 So, in that example, it makes a lot of  
22 sense to me, but on the other hand, I've been a part  
23 of retrofit or existing plant upgrades for a  
24 protection system or an ESFAS system. I've done  
25 a turbine control system. I've been a part of a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 process plant computer upgrade. That's a  
2 different situation and that doesn't apply the same  
3 as it does in doing a reactor protection system  
4 design.

5 So, I think that's -- I guess to boil  
6 this all down that's the challenge. Is -- we're  
7 talking about very specific scopes and how to  
8 understand how any changes would affect those  
9 scopes. I think specifically for the NuScale  
10 Power situation where we're designing attributes  
11 into the protection system to mitigate hazards, I  
12 think it makes a lot of sense for the staff to look  
13 at those as both malicious and non-malicious  
14 hazards and credit the designs that have been in  
15 place so that that can be carried forward  
16 throughout the full licensing process on into  
17 operating a plant and being programmatically  
18 implemented.

19 MR. PEZESHKI: First, I really wanted  
20 to thank you for your comments. You pretty much  
21 hit the nail on the head with what we were trying  
22 -- what we are trying to accomplish with Option 1  
23 and you put it very succinctly and I really do  
24 appreciate that.

25 The main reason for the wider scope was

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 really to achieve regulatory consistency across  
2 newer reactors and existing reactors. When  
3 putting this together, we were fully cognizant that  
4 this was not really a giant leap forward for the  
5 existing fleets, but simply just the sense of  
6 achieving consistency. It was I'll say the reason  
7 why we're going for -- considered cyber security  
8 as oppose to these are controls you must implement  
9 which would be insane and I think you can agree  
10 with that. What if we started specifying like you  
11 must have password protection on all your systems?  
12 No, that's nuts.

13 But consideration of access control  
14 with us accepting the fact that your answer may  
15 simply be that's going to be programmatic. We're  
16 going to leave that for programmatic. We've got  
17 a lovely room with a lock on it. We're fine.  
18 That's fine as well. It was considered.

19 But, yes, it's absolutely not going to  
20 have a tremendous impact on operating reactors.  
21 It's really directed to the reactors, but we don't  
22 want 52 to be completely different than Part 50.

23 MR. STATTEL: The staff had discussed  
24 one possibility of basically bifurcating this and  
25 making different regulations for operating versus

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 new reactors, but I'm really opposed to this idea.  
2 I think we need to be consistent. I mean, the new  
3 reactors become operating reactors and to have to  
4 deal with different sets or different criteria for  
5 a reactor depending on when it was designed and  
6 built, I think that's a burden that we would be  
7 pushing to the future that we would always regret.  
8 Okay.

9 So, we're really trying to push for some  
10 commonality and consistency between the operating  
11 and new reactors even though we recognize that the  
12 problems are very different for them.

13 MS. ZHANG: But if you have any  
14 suggestions of, you know, maybe not total  
15 bifurcation, but if there is something different  
16 we do for design certification applicants and COL  
17 applicants versus a license amendment request,  
18 then definitely we would like to hear that.

19 MR. BAILEY: Mike Bailey again with  
20 Duke Energy.

21 I think just from an overall  
22 standpoint, I think the last two points from new  
23 reactors as well as from the vendors pointed to a  
24 couple of things.

25 As you look through the wording and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 what's in Option 1 and two and three at this point  
2 in time and part of the reason, you know, because  
3 our industry discussions prior to the meeting  
4 involve utilities that had new reactors under  
5 development and also had existing plants as well.  
6 So, we looked at it from a consistency standpoint  
7 and the overall picture. The things that are  
8 stated right now are rather broad.

9 I think we've had some real good  
10 discussions about specific examples and I think we  
11 could probably get some alignment on specific  
12 examples and I think if as we have further  
13 discussions, if we can further define the scope,  
14 further define where these actual options are.  
15 The example on the new reactor side was very limited  
16 and very focused were the words used.

17 Whereas, the options currently  
18 presented are very broad and encompassing and so,  
19 from that standpoint, that was the one big concern  
20 we had from a new reactor as well as an operating  
21 reactor standpoint.

22 Where exactly do we land? If we say our  
23 feedback would be Option 1, then once we get into  
24 the details, we're really okay, well, okay, we  
25 really like Option 3 now. So, I think that's one

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 thing we probably need to have additional  
2 discussions on and get further details so we can  
3 actually get some of that alignment between both  
4 the NRC and the utility at that point.

5 MR. HERB: Again, one last thing, too,  
6 from the industry, from the existing industry,  
7 there's already a lot of uncertainty with digital  
8 systems and particularly digital in safety and I  
9 think that adding additional requirements  
10 inspections to consider malicious versus  
11 non-malicious when they really result in the same  
12 issues may just drive the industry to put in analog  
13 protection systems.

14 MR. GROSS: Which you can buy on eBay.  
15 It sounds to me digital's not really,  
16 you know, nuclear digital I guess is really sort  
17 of a strange beast that I don't really have a good  
18 understanding of, but it sounds like the measures  
19 and the guidance and the requirements that are in  
20 place today regarding access control for these I&C  
21 systems appear to be more than adequate for  
22 non-malicious acts.

23 Is that a true statement?

24 And the concern that we're addressing  
25 here is whether or not we should be integrating a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 treatment into the design to thwart or be able to  
2 defend against a malicious act against the I&C  
3 system for cyber security.

4 You know, the NRC's regulatory  
5 framework that incorporates cyber security is in  
6 its DBT requirements. Where a cyber attack is one  
7 attribute of the radiological sabotage design  
8 basis threat. So, it's one tool in the adversary's  
9 toolbox and I get a little concerned when we talk  
10 about now sort of having this standalone vision  
11 that cyber is somehow different and we need to treat  
12 it different.

13 My concern is if we start requiring  
14 licensees or providing clear expectations on how  
15 a licensee should incorporate or treat cyber  
16 security, i.e., how the safety system should defend  
17 itself against malicious acts just for cyber opens  
18 the door for us now to require the system to be  
19 designed to withstand a physical act within the DBT  
20 as well and I really do think that that is a --  
21 that's a tremendous change in the way the  
22 Commission has treated safety or, you know, the  
23 design of these facilities and the implementation  
24 of the cyber security program and the physical  
25 protection program.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           MR. STATTEL: I'm not sure I understand  
2 your point because I kind of disagree. I think our  
3 current policy is actually pretty consistent with  
4 the way we have treated, for instance, analog I&C  
5 systems in the past.

6           So, for example, we did not -- design  
7 engineers did not necessarily consider malicious  
8 acts or sabotage-type activities for designs of I&C  
9 systems back in the 1970s and the '80s.

10           However, the NRC did require security  
11 protection at the plant. So, the physical  
12 security was put into place and it was treated  
13 separately. It was treated as a separate entity.

14           So, the way I see it is the way we have  
15 separated this for cyber security for digital  
16 systems, it's actually pretty consistent with the  
17 way we treated these systems even before the  
18 digital systems were coming into play.

19           So, I'm not quite sure I understand your  
20 point.

21           MR. GROSS: I may have misstated. But  
22 you accurately characterized my concern. Which is  
23 there is and Reg Guide 1.152 Rev 3 makes a very clear  
24 demarcation between the safety system as designed,  
25 you know, up to this point to address non-malicious

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 acts and the Part 73 program as implemented to  
2 protect the system against malicious acts.

3 What I see in this paper is throwing all  
4 that out the window and saying design features  
5 should be incorporated into the I&C system so that  
6 it can withstand a malicious act just for cyber and  
7 that opens the door to do the same thing for  
8 physical and that's where I get concerned.

9 MS. ZHANG: We're not asking for that.  
10 It must be -- yes, it's not our intent to specify  
11 that cyber security features must be incorporated  
12 into the design, but if you were to consider cyber  
13 security earlier in the design process, you know,  
14 you can submit that information for NRC review.

15 I think it's similar for physical  
16 security, but I may be wrong. If they voluntarily  
17 submit physical security information, you know, we  
18 can review it.

19 MR. GROSS: Thank you.

20 MR. JONES: I think at this point why  
21 don't we take just ten minutes and what I'd like  
22 to do is come back and then get our industry  
23 participants on the bridge line who haven't yet had  
24 a chance to throw questions in here. Let's start  
25 to bring that in.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1           So, if we could come back at why don't  
2 we say 10:45. Thank you.

3           (Whereupon, the above-entitled matter  
4 went off the record at 10:34 a.m. and resumed at  
5 10:46 a.m.)

6           MR. JONES: Okay. Folks, we're going  
7 to try and bring in some questions on the phone from  
8 industry. It's going to be really, really  
9 difficult to hear them based on how hard it's been  
10 to hear the operator so far. So, if we could, let's  
11 listen for the question coming in. It's going to  
12 come in through the overhead and then somebody gets  
13 it or if I get it, we'll repeat the question and  
14 then we'll take off from there.

15           OPERATOR: Thank you. We will now  
16 begin the question and answer session. If you  
17 would like to ask a question, please press star-1.  
18 You will be prompted on the earphone to record your  
19 name and again, that's star-1 to ask a question from  
20 the phone lines.

21           We do have a question in the queue.

22           MR. JONES: Go ahead.

23           OPERATOR: Our first question comes  
24 from Mike Berube. Your line is now open, Mr.  
25 Berube.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 MR. JONES: Mr. Berube, please give  
2 your name and your affiliation.

3 MR. BERUBE: Yes, this is Mike Berube  
4 actually with GE Hitachi.

5 And a couple of things I wanted to  
6 mention. Earlier, you mentioned that for the  
7 ESPWR-certified design that our cyber program was  
8 not reviewed as part of the FSER and I'm looking  
9 at a section of that now, Chapter 7, that dealt  
10 specifically with the SDOE and our LPR for our cyber  
11 security program is mentioned in there many times  
12 and referenced several times in there as well as  
13 some additional LPRs that we have submitted and got  
14 NRC approval that relate to our software management  
15 plan and SQA plan.

16 So, the NRC is well aware of our efforts  
17 to integrate cyber security into the design of all  
18 the digital systems that make up ESPWR design.

19 MS. ZHANG: So, to answer that question  
20 --

21 MR. BERUBE: The other thing I wanted  
22 to point out was or ask a question was  
23 EPRI along with representatives from the industry  
24 has done a good job in putting together some cyber  
25 security procurement methodology and in there,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 they even point out the relevant NEI 08-09 or Reg  
2 Guide 5.71 controls that would apply or could --  
3 you know, a vendor could provide some added benefit  
4 to. Kind of a shared type of a responsibility and  
5 we are utilizing that guidance as we go forward.

6 So, I think some of what you're  
7 concerned about is kind of already being addressed  
8 in other areas and cyber definitely is being  
9 integrated into the design of the new plants going  
10 forward at least in our case.

11 MS. ZHANG: This Deanna Zhang. I'm  
12 going to respond to your questions.

13 For the first one, yes, we do recognize  
14 that the cyber security program plan that GEH  
15 submitted was reviewed, but it was only reviewed  
16 for the SDOE portion. There were clear statements  
17 that were written in the SER to state that it was  
18 not reviewed with respect to 10 CFR 73.54 for  
19 addressing malicious acts.

20 And for the --

21 MR. BERUBE: That's true. I agree  
22 with that. But I think that his statement earlier  
23 was that there was no cyber aspects at all in our  
24 review and that I just wanted to clarify.

25 MS. ZHANG: Yes, we just mean to

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 address malicious.

2 So, for the second point, we do  
3 recognized that industry vendors are taking  
4 measures to address cyber security early, but those  
5 measures would not be able to be reviewed by the  
6 NRC if that was desired by the design certification  
7 applicant or licensee.

8 So, we're just looking at means to  
9 perform that licensing review so that you can get  
10 a safety evaluation on those particular features  
11 with respect to malicious acts.

12 MR. JONES: Next question please.

13 OPERATOR: Our next question comes  
14 from Ken Scarola. Your line is now open.

15 MR. SCAROLA: Yes, thank you. My name  
16 is Ken Scarola from Nuclear Automation  
17 Engineering.

18 I just wanted to make a comment. I  
19 really don't have a question.

20 And I just wanted to say that many of  
21 you have probably seen my presentations or maybe  
22 -- or maybe you have heard my discussions about the  
23 obstacles to analog to digital migration.

24 And the most significant of those is the  
25 unpredictable costs of what digital systems really

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 take to install and I think everyone knows the  
2 changes that occur late in the design project for  
3 any reason and that would include a cyber security  
4 inspection at the plant can be detrimental to cost.

5 So, having an NRC review very early in  
6 the project is essential to achieve cost  
7 predictability and this is especially important  
8 when you have systems that include non-safety to  
9 safety by directional data communication.

10 So, I am fully supportive of what I've  
11 heard in this meeting today. I think the NRC or  
12 NRR and the NRO should be reviewing these safety  
13 systems designs for adequate cyber security  
14 measures.

15 That's my first comment. Just I'm very  
16 supportive of this.

17 Second, I wanted to emphasize the  
18 importance of what I heard from Rich Stattel about  
19 needing to have the same regulations and the same  
20 guidance for both new plants and operating plants.  
21 It can be really confusing downstream if we don't  
22 have the same guidance because as Rick said a new  
23 plant becomes an operating plant.

24 Therefore, it just makes no sense to me  
25 that we wouldn't even think about having different

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



1 regulations or different guidance.

2 That's all I have to say. Thank you.

3 MR. JONES: Thank you. Next question.

4 OPERATOR: And again, if you would like  
5 to ask a question, please press star-1. You will  
6 be prompted to leave your phone number, record your  
7 name and again, that's star-1 to ask a question.

8 And at this time, I'm showing no  
9 questions in queue.

10 MR. JONES: Okay. Would you put  
11 everyone back on listen only, please?

12 OPERATOR: Sure.

13 MR. JONES: Okay. Deanna, back to  
14 you.

15 MS. ZHANG: Again, I would like to  
16 thank you guys for coming here and for those who  
17 are participating on the phone. I think we've  
18 heard some pretty good feedback from everyone here  
19 and we would like to continue to engage industry  
20 in gaining more feedback from you as we progress  
21 in our -- in the development of our SECY paper.

22 MR. JONES: One last comment, if we're  
23 through with the industry NRC discussion, we need  
24 to offer the public a chance if there's anyone on  
25 the line. So, let me try that again.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 Operator, are you still there?

2 OPERATOR: Yes, I'm here. We do have  
3 a couple of questions in queue and one moment  
4 please.

5 Our first question come from Kelly  
6 Deopani (phonetic).

7 MR. DEOPANI: Hello. This is Kelly  
8 Deopani from I&C Engineering, GE Hitachi.

9 The question I have is regarding  
10 performing static and dynamic analysis. My  
11 understanding is that performance of static and  
12 dynamic analysis is a security requirement. How  
13 the NRC will insure that this requirement is  
14 precisely implemented? So, this maybe goes under  
15 Option 1. After you identify the security  
16 requirements, you still need to perform some  
17 programmatic controls like performing static and  
18 dynamic analysis and the static and dynamic  
19 analysis are listed under 5.71, Reg Guide 5.71.

20 So, how does the NRC plan to enforce  
21 this requirement?

22 MR. PEZESHKI: Thank you. This is  
23 Jonah Pezeshki, NSIR.

24 So, first, I just want to state that the  
25 Option 1 that we've described that talks about

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 design level cyber security requirements is not  
2 intended to replace the current programmatic cyber  
3 security requirements nor the cyber security  
4 inspections that would occur after implementation.

5 So, to answer your question, those  
6 systems would still be subject to the cyber  
7 security programmatic level requirements and the  
8 corresponding inspections.

9 MR. DEOPANI: All right. Thank you.

10 MR. JONES: Next question please.

11 OPERATOR: Next question comes from  
12 Mark. Your line is now open.

13 MR. KING: Thank you. In the  
14 presentation materials --

15 MR. JONES: Mark, would you please give  
16 your name and your affiliation or general public?

17 MR. KING: Mark King, NuScale Power.

18 In the presentation, it indicates one  
19 section of Reg Guide 5.71, Section D.1.4 that would  
20 possibly be included during DCA.

21 Are there thoughts on entertaining or  
22 are you entertaining thoughts on any other sections  
23 being applicable? For instance, Appendix C,  
24 Section C.12.5 regarding some very specific things  
25 that the licensee would today be required to insure

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 of their contractors or vendors.

2 MS. ZHANG: That one was particularly  
3 called out because it addressed the defense  
4 architecture and the boundary device between the  
5 different security levels of the cyber security  
6 defense architecture. So, it was very specific to  
7 Option 2.

8 We have not looked at the wide range of  
9 security controls in Reg Guide 5.71 and done a 141  
10 analysis of what we would look at. So, that's  
11 something we would consider in the -- as we were  
12 developing the SECY paper. More -- you know, and  
13 also as we -- if we were told that we can go proceed  
14 with rulemaking, then, you know, we would probably  
15 look at it in more detail, too.

16 MR. KING: Because some of those are  
17 specifically activities that would start during  
18 design time. So, it would seem appropriate.

19 MS. ZHANG: Yes, we understand. It's  
20 more specific to the procurement specifications  
21 addressing development. The development of  
22 systems.

23 MR. KING: Okay. Thank you.

24 MR. JONES: Next question please.

25 OPERATOR: Our next question comes

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 from Mike Berube. Your line is now open.

2 MR. BERUBE: Yes, this is Mike Berube  
3 from GE Hitachi again.

4 Just as a follow-up from earlier and I  
5 think it's been brought up a few times, this  
6 difference between non-malicious and malicious  
7 acts.

8 Does the NRC have a definition of their  
9 scope of what they are going to consider malicious  
10 acts that would need to be protected against and  
11 incorporate into the design?

12 MS. ZHANG: I think we just called the  
13 cyber threat as defined in 73.1. I believe it's  
14 the design basis threat.

15 So, I don't know if NSIR would like to  
16 add anything else. Okay. No.

17 MR. BERUBE: So, are there specific  
18 criteria in 73.1 that they are spelled out?

19 MS. ZHANG: I don't think so.

20 MR. BERUBE: So, that would need to be  
21 defined then as part of that SECY paper I assume?

22 MS. ZHANG: Maybe as part of the role.  
23 We have -- I don't know if we -- yes, I don't think  
24 we would probably be defining that as part of the  
25 SECY paper.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 MR. BERUBE: Okay. Well, that is  
2 obviously important because if we don't know what  
3 is considered a malicious act, then we don't know  
4 what to protect against.

5 MR. PEZESHKI: Oh, I just wanted to  
6 clarify. In this case, the SECY paper would be a  
7 request from the Commission to proceed with  
8 rulemaking.

9 The specifics of what would be  
10 considered a malicious act and the specific  
11 controls would be considered once we get permission  
12 to proceed with rulemaking as a part of the  
13 rulemaking effort.

14 MS. ZHANG: But, currently, you know,  
15 to address the cyber threat, I think licensees  
16 understand what they need to protect against from  
17 a cyber attack. So, you know, I don't know what  
18 else we need to define in that case.

19 MR. BERUBE: So, you're saying to the  
20 licensees what characterizes a malicious act is  
21 already defined? So, can we just adopt that?  
22 Where would I look for that?

23 MS. ZHANG: Seventy-three point two.

24 MR. BERUBE: Okay.

25 MR. JONES: Thank you. Next question.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 OPERATOR: Again, if you would like to  
2 ask a question, please press star-1.

3 MR. JONES: Okay. Hearing no other  
4 questions, I guess we'll conclude the meeting.

5 Thank you for coming and I want to point  
6 out that there are public meeting feedback forms  
7 here on the table or you can get them online  
8 underneath the public meeting notice and it's an  
9 attachment to the notice.

10 Any other final comments? Then we're  
11 done. Thank you.

12 MS. ZHANG: Thank you.

13 (Whereupon, the above-entitled matter  
14 was concluded at 11:02 a.m.)

15

16

17

18

19

20

21

22

23

24

25

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1  
2  
3  
4  
5  
6